МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

Кваліфікаційна наукова
праця на правах рукопису

БОНДАР ДМИТРО ВОЛОДИМИРОВИЧ

УДК 342.92

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Подається на здобуття наукового ступеня **доктора юридичних наук**

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Д.В. Бондар

Ужгород – 2025

АНОТАЦІЯ

Бондар Д.В. Адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук зі спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – ДВНЗ «Ужгородський національний університет», Ужгород, 2025.

Дисертацію присвячено комплексному дослідженню адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Проаналізовано рівень наукового розроблення проблематики теоретико-методологічних засад та стану адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Акцентовано увагу на тому, що, незважаючи на те, що питання теоретико-методологічних засад та адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності частково входили до предмета багатьох наукових праць, присвячених правовому регулюванню систем забезпечення життєдіяльності та цивільного захисту, а також їх теоретико-методологічним засадам, пошуки в цьому напрямі не можна вважати вичерпаними.

По-перше, більшість наукових напрацювань стосуються правового регулювання забезпечення цивільного захисту та безпеки життєдіяльності в цілому, а не сутності комплексного механізму адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. По-друге, в адміністративному праві недостатньо представлене доктринальне обґрунтування необхідності адміністративно-правового забезпечення використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. По-третє, сформувалося чимало

дискусійних аспектів у розумінні сутності адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а саме ролі органів публічної адміністрації та системи адміністративно-правових засобів забезпечення ефективної діяльності суб'єктів владних повноважень, спрямованої на забезпечення безпеки життєдіяльності та цивільного захисту населення та територій від надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру. По-четверте, наявні проблемні питання адаптації національного адміністративного законодавства до права ЄС у даній сфері суспільних відносин. По-п'яте, очевидною є потреба розробки та прийняття Закону України «Про штучний інтелект», в якому буде регламентовано різні аспекти використання технології штучного інтелекту, включаючи його використання у сфері забезпечення безпеки життєдіяльності. По-шосте, об'єктивною є потреба прийняття спільного наказу МВС України та Міністерства цифрової трансформації України про затвердження порядку використання Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку, що дозволить оперативно мобілізувати людські та матеріально-технічні ресурси для ліквідації надзвичайних ситуацій та їх наслідків.

Вищевикладене актуалізує необхідність глибокого теоретичного опрацювання проблемних питань адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, з урахуванням міжнародних стандартів, норм та принципів права ЄС.

Проаналізовано поняття та правову природу систем забезпечення безпеки життєдіяльності та цивільного захисту. Сформульовано авторське визначення безпеки життєдіяльності в контексті цифровізації як комплексної науки та навчальної дисципліни, яка досліджує всі негативні чинники (небезпеки), які вливають або потенційно можуть вплинути на життєдіяльність людини в сучасному інформаційному суспільстві, порушити порядок нормального функціонування та розвитку суспільства в цілому,

встановлює систему технічних та техніко-юридичних норм взаємодії людини із навколишнім середовищем та цифровим світом, а також визначає систему засобів запобігання та протидії вказаним негативним чинникам (небезпекам), ліквідації надзвичайних ситуацій та їх наслідків, включаючи інноваційні інформаційні технології, використання яких потребує належної адміністративно-правової регламентації.

Встановлено, що безпека життєдіяльності є більш широким поняттям ніж цивільний захист, і включає останній наряду із системами забезпечення охорони праці, безпечності харчових продуктів та продовольчої сировини, безпеки дорожнього руху тощо.

Проаналізовано основні групи наукових методів та методологічних підходів, які необхідно використовувати для дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Особлива увага приділена законам та прийомам діалектики (єдності та боротьби протилежностей, переходу кількісних змін у якісні, прийом «заперечення заперечення») як універсального методу наукової роботи.

Встановлено, що прийом «заперечення заперечення» використовується у сфері адміністративно-правового регулювання систем забезпечення безпеки життєдіяльності та цивільного захисту в процесі визначення суспільних відносин, які потребують правового регулювання. Підкреслено, що технічні норми, які становлять більшу частину правил безпеки життєдіяльності не здатні самі по собі забезпечити їх дотримання і тільки санкціонування державою, надання технічним нормам правової визначеності дозволяє певною мірою гарантувати їх дотримання усіма учасниками суспільних відносин. В якості прикладів наведено норми щодо охорони праці, безпечності харчових продуктів та продовольчої сировини, Правила дорожнього руху.

В свою чергу адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволяє уніфікувати, стандартизувати програмне забезпечення, яке

використовується різними органами публічної адміністрації (що гарантує сумісність цифрових технологій в процесі їх використання), забезпечити централізований захист інформаційних ресурсів у сфері забезпечення безпеки життєдіяльності та цивільного захисту, а також поширити локальний позитивний досвід використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності на територію всієї держави.

Закон переходу кількісних змін у якісні проявляється в процесі поступової, методичної адміністративно-правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Збільшення кількості адміністративно-правових актів, які регулюють різні аспекти вказаних суспільних відносин, напрацювання адміністративної та судової практики рано чи пізно призводить до якісних змін – появи чітких, регламентованих алгоритмів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а також підвищення ефективності відповідних цифрових продуктів та послуг.

Нарешті закон єдності та боротьби протилежностей дозволяє зіставити всі негативні та позитивні чинники, які впливають на безпеку життєдіяльності в процесі цифровізації суспільних відносин та розвитку інформаційного суспільства в цілому. В якості прикладу наведено позитивні аспекти та загрози, пов’язані із використанням технології штучного інтелекту в механізмах забезпечення безпеки життєдіяльності та цивільного захисту.

Акцентовано увагу на необхідності застосування різних наукових підходів для дослідження проблематики адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а саме, інструментального, цивілізаційного, антропологічного, телеологічного, аксіологічного та синергетичного.

Проаналізовано основні етапи становлення доктрини адміністративного права щодо проблематики адміністративно-правової регламентації систем забезпечення безпеки життєдіяльності та цивільного захисту, включаючи

використання інформаційних технологій у вказаній сфері суспільних відносин.

Виділено основні етапи становлення та розвитку інформаційного суспільства (цифровізації) в контексті забезпечення безпеки життєдіяльності та використання інформаційних технологій в єдиній державній системі цивільного захисту.

Підкреслено важливість поступового нормативного врегулювання та економічного (матеріально-технічного) забезпечення використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

В історії цифровізації діяльності органів публічної адміністрації, включаючи впровадження інформаційних технологій в діяльність Державної служби України з надзвичайних ситуацій, виділено чотири основних етапи, останній з яких характеризується активним впровадженням інноваційних інформаційних технологій у сферу забезпечення безпеки життєдіяльності та цивільного захисту, що включає: використання технології штучного інтелекту та можливостей мобільних застосунків, створення автоматизованих інтегрованих інформаційних систем цивільного захисту тощо.

Показано, що порядок функціонування національних систем забезпечення безпеки життєдіяльності та цивільного захисту врегульовано ієрархією нормативно-правових актів, включаючи Конституцію України, ратифіковані міжнародні договори, кодекси та закони України, укази Президента України та постанови Кабінету Міністрів України, накази органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, спільні накази органів публічної адміністрації з питань цивільного захисту та безпеки життєдіяльності в різних сферах суспільних відносин, акти органів місцевого самоврядування, а також судову практику, зокрема, правові позиції (висновки) Верховного Суду та касаційних судів у складі Верховного Суду.

Окрему увагу приділено актуальним питанням адміністративно-правового забезпечення діяльності органів публічної адміністрації у сфері

забезпечення життєдіяльності, включаючи єдину державну систему цивільного захисту.

Особливістю адміністративно-правого регулювання у сферах забезпечення безпеки життєдіяльності та цивільного захисту названо достатньо часту спільну нормотворчість органів публічної адміністрації з метою забезпечення обміну інформацією про надзвичайні ситуації та координації діяльності з ліквідації надзвичайних ситуацій та їх наслідків. Ще однією особливістю названо часте використання техніко-юридичних (технічних) норм в підзаконних актах.

Підкреслено необхідність адміністративно-правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності з метою забезпечення сумісності програмного забезпечення, централізованого захисту інформації та поширення позитивного досвіду використання інноваційних інформаційних технологій у вказаній сфері суспільних відносин.

Встановлено, що заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій достатньо детально регламентовані Кодексом цивільного захисту України та Законом України «Про правовий режим надзвичайного стану». Крім того, вказані заходи передбачені підзаконними нормативно-правовими актами, серед яких: Концепція захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій, схвалена указом Президента України від 26 березня 1999 р. № 284/99, Положення про Державну службу України з надзвичайних ситуацій, затверджене постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1052, Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв’язку у сфері цивільного захисту, затверджене постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733.

За результатами дослідження системи суб’єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності

сформульовано висновок про те, що, враховуючи зростаючі загрози природнього, техногенного, соціального та воєнного характеру, існує реальна потреба створення єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати інтерактивну мапу та інформаційну базу суб'єктів забезпечення цивільного захисту. Також існує об'єктивна потреба нормативного визначення системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які будуть здійснювати адміністрування вказаної інформаційно-телекомунікаційної системи, відповідної бази даних, а також здійснювати оперативне обслуговування (керування центром управління, штабом) мобільних застосунків, призначених для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації.

Вказано на необхідність внесення змін до чинного національного законодавства щодо адміністративно-правової регламентації створення єдиної інформаційно-телекомунікаційної системи цивільного захисту, а також адміністративно-правової регламентації використання мобільних застосунків у сфері забезпечення безпеки життєдіяльності, включаючи права та обов'язки суб'єктів, які будуть здійснювати адміністрування вказаних мобільних застосунків, а також суб'єктів, які будуть залучатися до ліквідації надзвичайних ситуацій та їх наслідків в якості добровольців з використанням встановленого мобільного застосунку.

Підкреслено, що правового врегулювання потребує і питання фінансового та матеріально-технічного забезпечення функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб'єктів, які на добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків.

За результатами дослідження досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі встановлено, що в Механізмі цивільного захисту Європейського Союзу використовуються такі інформаційні технології як інформаційні платформи, бази даних, засоби оперативного зв'язку та координації тощо. Використання вказаних інформаційних технологій має належну правову регламентацію на рівні рішень Європейського парламенту та Європейської Ради.

До правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності віднесено GDPR – Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних, а також Європейський закон (Регламент) про штучний інтелект (Artificial Intelligence Act, AI Act). Важливими документами щодо регулювання розвитку цифровізації в Європейському Союзі також є Європейська структура сумісності (EIF), яка надає загальний набір стандартів для забезпечення легкого доступу до державних послуг і спільного використання в усьому ЄС, а також Регламент eIDAS, що визначає правила електронної ідентифікації та довірчих послуг у всьому ЄС.

Зазначено, що Міністерству цифрової трансформації України, необхідно активізувати участь національних державних та приватних інституцій у розвитку Єдиного цифрового ринку ЄС, залучати інвестиції для розвитку національного цифрового ринку, включаючи фінансування заходів із забезпечення кібербезпеки. Крім того, одним із завдань є завершення процедур адаптації національного законодавства в частині правового регулювання використання інформаційних технологій та забезпечення безпеки життєдіяльності до права ЄС.

Сформулювано висновок про можливість та доцільність запозичення позитивного досвіду органів публічної адміністрації США в частині адміністративно-правової регламентації діяльності у сфері цивільного захисту

населення і територій від надзвичайних ситуацій. Зокрема, до позитивного досвіду віднесено розробку та реалізацію FEMA Федерального плану, який є головним актом у процесі реагування на надзвичайну ситуацію та ліквідацію її наслідків. Також позитивним названо досвід побудови структури та організації діяльності Федерального агентства з управління надзвичайними ситуаціями (FEMA), зокрема його функції щодо адміністрування та координації діяльності інших органів публічної адміністрації у вказаній сфері суспільних відносин.

Вказано на доцільність запозичення структури та змісту офіційного сайту FEMA, який містить детальну інформацію як для суб'єктів владних повноважень, так і для громадян щодо організації цивільного захисту населення та територій США від надзвичайних ситуацій.

Звернуто увагу на досвід FEMA у сфері координації діяльності органів публічної адміністрації щодо своєчасного реагування на надзвичайні ситуації та оперативної ліквідації їх негативних наслідків, а також акумулювання інформації про надзвичайні ситуації, що забезпечується засобами комунікації з використанням новітніх інноваційних інформаційних технологій (швидкісного оптоволоконного зв'язку, захищеного серверного обладнання, хмарних технологій, можливостей соціальних мереж та месенджерів, технології штучного інтелекту тощо).

Зазначено, що позитивний досвід США щодо розроби та реалізації федерального плану реагування на надзвичайні ситуації імплементовано в національне законодавство на рівні постанови Кабінету Міністрів України від 14 березня 2018 р. № 223 «Про затвердження Плану реагування на надзвичайні ситуації державного рівня», що дозволяє національним органам публічної адміністрації оперативно реагувати на надзвичайні ситуації.

Підкреслено доцільність запозичення трирівневної системи публічного управління ліквідацією надзвичайних ситуацій та їх наслідків в Японській Державі, в якій ключову роль відіграє рівень муніципалітетів, тобто організація сил та засобів цивільного захисту на рівні органів місцевого

самоврядування, що дозволяє максимально оперативно реагувати на початок надзвичайної ситуації, а також проводити систематичні навчання та тренінги із населенням у сфері цивільного захисту.

Показано сталість національного законодавства Японії та стабільність (традиціоналізм) функціонування органів публічної адміністрації, які реалізують державну політику Японської Держави у сфері забезпечення пожежної безпеки. Зазначається, що цей досвід вартий запозичення Україною, адже постійні реформи центральних органів виконавчої влади, включаючи органи публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, не сприяють їх ефективній роботі, що включає формування традицій, злагодженості та згуртованості колективів, внутрішньої субкультури тощо.

Названо позитивним досвід Японської Держави щодо створення «муніципальних корпорацій» або «асоціацій районів» з метою консолідації фінансових та організаційних ресурсів для ліквідації надзвичайних ситуацій. Також позитивним є досвід щодо функціонування волонтерських пожежних корпусів, які складаються із пожежних-волонтерів, які мають власну трудову діяльність або зайнятті на іншій найманій роботі (однак у разі пожежі або іншої надзвичайної посадові особи та інші члени волонтерських пожежних корпусів повинні дотримуватися розпоряджень начальника пожежного департаменту або пожежної станції).

Звернуто увагу на ізраїльську національну безпекову доктрину, ефективність існування якої підтверджена під час захисту цивільного населення в умовах воєнного протистояння, що постійно триває. Для України, яка знаходиться у схожій ситуації, актуальною є ізраїльська модель поєднання сил та засобів органів військового управління та цивільних органів публічної адміністрації в організації ліквідації надзвичайних ситуацій та їх наслідків, включаючи використання сучасних інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а саме новітніх систем оповіщення цивільного населення про загрозу ракетних обстрілів. Воєнно-орієнтований

підхід до управління в умовах кризових ситуацій в Ізраїлі заслуговує на більш детальне дослідження та імплементацію в національне законодавство та юридичну практику.

Також виокремлено позитивний досвід Держави Ізраїль щодо залучення добровольців-пожежників для ліквідації надзвичайних ситуацій.

За результатами дослідження актуальних напрямів удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності виділено наступні перспективні напрями нормотворчої діяльності у вказаній сфері суспільних відносин:

- адміністративно правове врегулювання розробки та функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати, серед іншого, інтерактивну мапу захисних укриттів (з можливістю побудови маршруту слідування для особи з урахуванням геолокації), місць локалізації надзвичайних ситуацій та їх наслідків (за виключенням місць прильотів ворожих ракет та безпілотних літальних апаратів), а також інформаційну базу суб'єктів забезпечення цивільного захисту та безпеки життєдіяльності;

- адміністративно-правова регламентація розробки, поширення (популяризації), а також порядку адміністрування і використання мобільного застосунку, призначеного для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації, а саме, затвердження спільним наказом МВС України та Міністерства цифрової трансформації України порядку використання Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку, що сприятиме залученню соціально-активних громадян до ліквідації надзвичайних ситуацій та їх наслідків;

- адміністративно-правове визначення системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які будуть здійснювати адміністрування єдиної інформаційно-телекомунікаційної

системи цивільного захисту, а також здійснювати оперативне обслуговування (керування центром управління) мобільних застосунків, призначених для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації;

- адміністративно-правове врегулювання питання фінансового та матеріально-технічного забезпечення функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб'єктів, які на добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків;

- прийняття окремого Закону України «Про штучний інтелект», яким будуть врегульовані, у тому числі, основні питання використання технології штучного інтелекту в єдиній державній системі цивільного захисту та в механізмі забезпечення безпеки життєдіяльності в цілому, а також адміністративно-правове врегулювання порядку використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності на рівні підзаконних (відомчих) нормативно-правових актів;

- адміністративно-правову регламентацію збереження важливої інформації у сфері цивільного захисту та забезпечення безпеки життєдіяльності на декількох альтернативних серверах, включаючи сервери, які розташовані в зарубіжних країнах, що мають надійні партнерські відносини з Україною;

- адміністративно-правову регламентацію використання робототехніки, яка здатна замінити людину в процесі ліквідації особливо небезпечних надзвичайних ситуацій та їх наслідків;

- встановлення адміністративної відповідальності за невиконання встановленого порядку поведінки під час оголошення повітряної тривоги в публічних місцях, на підприємствах, установах та організаціях, незалежно від

форми власності, що потребує внесення змін до чинного Кодексу України про адміністративні правопорушення та затвердження перспективного Порядку поведінки в публічних місцях, на підприємствах, установах та організаціях, незалежно від форми власності, під час повітряної тривоги.

Вказаний перелік не є вичерпним, адже в сучасному цифровізованому суспільстві майже щодня з'являються нові інформаційні технології, окремі з яких можуть бути використані у сфері забезпечення безпеки життєдіяльності та, відповідно, потребуватимуть належного адміністративно-правового регулювання.

Ключові слова: автоматизовані системи, адміністративно-правові засади, безпека життєдіяльності, запобігання, інформаційні технології, ліквідація, мобільні застосунки, надзвичайні ситуації, правове регулювання, цивільний захист, штучний інтелект.

ANNOTATION

Bondar D.V. Administrative and legal regulation of the use of information technologies in the field of ensuring life safety. – Qualification scientific work on the rights of the manuscript.

The dissertation for obtaining a scientific degree of doctor of legal sciences in the specialty 12.00.07 – administrative law and process; financial law; information law. – Uzhhorod National University, Uzhhorod, 2025.

The dissertation is devoted to a comprehensive study of the administrative and legal regulation of the use of information technologies in the field of ensuring life safety. The level of scientific development of the issues of theoretical and methodological principles and the state of administrative and legal regulation of the use of information technologies in the field of ensuring life safety is analyzed. Attention is focused on the fact that, despite the fact that the issues of theoretical and methodological principles and administrative and legal regulation of the use of information technologies in the field of ensuring life safety were partially included

in the subject of many scientific works devoted to the legal regulation of life safety and civil protection systems, as well as their theoretical and methodological principles, searches in this direction cannot be considered exhausted.

Firstly, most scientific works concern the legal regulation of ensuring civil protection and life safety in general, and not the essence of the complex mechanism of administrative and legal regulation of the use of information technologies in the field of ensuring life safety. Secondly, the administrative law does not sufficiently present the doctrinal justification of the need for administrative and legal support for the use of information technologies in the field of ensuring the safety of life. Thirdly, many debatable aspects have been formed in understanding the essence of administrative and legal regulation of the use of information technologies in the field of ensuring the safety of life, namely the role of public administration bodies and the system of administrative and legal means of ensuring the effective activities of subjects of power aimed at ensuring the safety of life and civil protection of the population and territories from emergencies of a natural, technogenic, social and military nature. Fourthly, there are problematic issues of adapting national administrative legislation to EU law in this area of public relations. Fifthly, there is an obvious need to develop and adopt the Law of Ukraine «On Artificial Intelligence», which will regulate various aspects of the use of artificial intelligence technology, including its use in the field of ensuring the safety of life. Sixth, there is an objective need to adopt a joint order of the Ministry of Internal Affairs of Ukraine and the Ministry of Digital Transformation of Ukraine on approving the procedure for using the Alert and Response System «I am a Volunteer» and the corresponding mobile application, which will allow for the prompt mobilization of human and material and technical resources to eliminate emergencies and their consequences.

The above highlights the need for in-depth theoretical study of problematic issues of administrative and legal regulation of the use of information technologies in the field of ensuring life safety, taking into account international standards, norms and principles of EU law.

The concept and legal nature of life safety and civil protection systems are analyzed. The author's definition of life safety in the context of digitalization is formulated as a comprehensive science and academic discipline that studies all negative factors (dangers) that affect or can potentially affect human life in the modern information society, disrupt the normal functioning and development of society as a whole, establishes a system of technical and technical-legal norms of human interaction with the environment and the digital world, and also defines a system of means of preventing and counteracting the specified negative factors (dangers), eliminating emergencies and their consequences, including innovative information technologies, the use of which requires proper administrative and legal regulation.

It is established that life safety is a broader concept than civil protection, and includes the latter along with systems for ensuring labor protection, food safety and food raw materials, road safety, etc.

The main groups of scientific methods and methodological approaches that must be used to study the administrative and legal regulation of the use of information technologies in the field of ensuring life safety are analyzed. Special attention is paid to the laws and techniques of dialectics (unity and struggle of opposites, the transition of quantitative changes into qualitative ones, the technique of «denial of denial») as a universal method of scientific work.

It is established that the technique of «denial of denial» is used in the field of administrative and legal regulation of systems for ensuring life safety and civil protection in the process of determining social relations that require legal regulation. It is emphasized that technical regulations, which constitute the majority of life safety rules, are not capable of ensuring their compliance by themselves and only state sanctioning, providing technical regulations with legal certainty allows to a certain extent to guarantee their compliance by all participants in public relations. Examples include regulations on labor protection, food safety and food raw materials, and traffic regulations.

In turn, administrative and legal regulation of the use of information technologies in the field of ensuring life safety allows to unify, standardize software used by various public administration bodies (which guarantees the compatibility of digital technologies in the process of their use), to ensure centralized protection of information resources in the field of ensuring life safety and civil protection, and to spread local positive experience in the use of information technologies in the field of ensuring life safety throughout the territory of the entire state.

The law of the transition of quantitative changes into qualitative ones is manifested in the process of gradual, methodical administrative and legal regulation of the use of information technologies in the field of ensuring the safety of life. An increase in the number of administrative and legal acts that regulate various aspects of the specified social relations, the development of administrative and judicial practice sooner or later leads to qualitative changes - the emergence of clear, regulated algorithms for the use of information technologies in the field of ensuring the safety of life, as well as increasing the efficiency of relevant digital products and services.

Finally, the law of unity and struggle of opposites allows us to compare all the negative and positive factors that affect the safety of life in the process of digitalization of social relations and the development of the information society as a whole. For example, these are the positive aspects and threats associated with the use of artificial intelligence technology in the mechanisms of ensuring the safety of life and civil protection.

Attention is focused on the need to apply various scientific approaches to studying the issues of administrative and legal regulation of the use of information technologies in the field of ensuring life safety, namely, instrumental, civilizational, anthropological, axiological and synergistic.

The main stages of the formation of the doctrine of administrative law regarding the issues of administrative and legal regulation of systems for ensuring life safety and civil protection, including the use of information technologies in the specified area of public relations, are analyzed.

The main stages of the formation and development of the information society (digitalization) in the context of ensuring life safety and the use of information technologies in a unified state civil protection system are highlighted.

The importance of gradual regulatory regulation and economic (material and technical) support for the use of information technologies in the field of ensuring life safety is emphasized.

In the history of digitalization of the activities of public administration bodies, including the introduction of information technologies into the activities of the State Emergency Service of Ukraine, four main stages have been identified, the last of which is characterized by the active introduction of innovative information technologies into the sphere of ensuring life safety and civil protection, which includes: the use of artificial intelligence technology and the capabilities of mobile applications, the creation of automated integrated civil protection information systems, etc.

It is shown that the procedure for the functioning of national systems for ensuring the safety of life and civil protection is regulated by a hierarchy of regulatory legal acts, including the Constitution of Ukraine, ratified international treaties, codes and laws of Ukraine, decrees of the President of Ukraine and resolutions of the Cabinet of Ministers of Ukraine, orders of public administration bodies that implement state policy in the field of civil protection, joint orders of public administration bodies on issues of civil protection and safety of life in various spheres of public relations, acts of local self-government bodies, as well as judicial practice, in particular, legal positions (conclusions) of the Supreme Court and cassation courts within the Supreme Court.

Special attention is paid to topical issues of administrative and legal support for the activities of public administration bodies in the field of ensuring life, including a unified state system of civil protection.

A feature of administrative and legal regulation in the areas of ensuring life safety and civil protection is the fairly frequent joint rulemaking of public administration bodies in order to ensure the exchange of information about

emergencies and coordination of activities to eliminate emergencies and their consequences. Another feature is the frequent use of technical and legal (technical) norms in subordinate legislation.

The need for administrative and legal regulation of the use of information technologies in the area of ensuring life safety is emphasized in order to ensure software compatibility, centralized information protection and the dissemination of positive experience in the use of innovative information technologies in this area of public relations.

It is established that measures to ensure the safety of the population and territories in the event of emergencies are regulated in sufficient detail by the Civil Protection Code of Ukraine and the Law of Ukraine «On the Legal Regime of a State of Emergency». In addition, the above measures are provided for by subordinate regulatory legal acts, including: The Concept of Protection of the Population and Territories in the Event of Threats and Emergencies, approved by Decree of the President of Ukraine dated March 26, 1999 № 284/99, the Regulation on the State Emergency Service of Ukraine, approved by Resolution of the Cabinet of Ministers of Ukraine dated December 16, 2015 № 1052, the Regulation on Organizing Notification of Threats or Emergencies and Organizing Communications in the Field of Civil Protection, approved by Resolution of the Cabinet of Ministers of Ukraine dated September 27, 2017 № 733.

Based on the results of the study of the system of subjects using information technologies in the field of ensuring life safety, the conclusion was formulated that, taking into account the growing threats of a natural, man-made, social and military nature, there is a real need to create a single information and telecommunications system of civil protection, which will include an interactive map and an information base of subjects providing civil protection. There is also an objective need for a normative definition of the system of subjects using information technologies in the field of ensuring life safety, which will administer the specified information and telecommunications system, the corresponding database, as well as carry out operational maintenance (management of the control center, headquarters) of mobile

applications intended for the mobilization of human and material and technical resources in the event of a threat of occurrence or the immediate occurrence of an emergency.

It is indicated that there is a need to amend the current national legislation regarding the administrative and legal regulation of the creation of a unified information and telecommunications system for civil protection, as well as the administrative and legal regulation of the use of mobile applications in the field of ensuring the safety of life, including the rights and obligations of entities that will administer the specified mobile applications, as well as entities that will be involved in the elimination of emergencies and their consequences as volunteers using the installed mobile application.

It is emphasized that legal regulation is also required for the issue of financial and logistical support for the functioning of the unified information and telecommunications system for civil protection, a mobile application for the mobilization of human and logistical resources in the event of a threat of or the immediate occurrence of an emergency, as well as the issue of financial and logistical support for entities that will be involved in the elimination of emergencies and their consequences on a voluntary basis.

According to the results of a study of the experience of administrative and legal regulation of the use of information technologies in the field of ensuring the safety of life in the European Union, it was established that the European Union Civil Protection Mechanism uses such information technologies as information platforms, databases, means of operational communication and coordination, etc. The use of these information technologies has appropriate legal regulation at the level of decisions of the European Parliament and the European Council.

The legal basis for the use of information technologies in the field of ensuring the safety of life includes GDPR – Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as the European Law (Regulation) on artificial intelligence (Artificial Intelligence Act,

AI Act). Important documents regulating the development of digitalization in the European Union are also the European Interoperability Framework (EIF), which provides a common set of standards to ensure easy access to public services and shared use throughout the EU, as well as the eIDAS Regulation, which defines the rules for electronic identification and trust services throughout the EU. It is noted that the Ministry of Digital Transformation of Ukraine needs to intensify the participation of national public and private institutions in the development of the EU Single Digital Market, attract investments for the development of the national digital market, including financing measures to ensure cybersecurity. In addition, one of the tasks is to complete the procedures for adapting national legislation in terms of legal regulation of the use of information technologies and ensuring the safety of life to EU law.

A conclusion is formulated on the possibility and expediency of borrowing the positive experience of US public administration bodies in terms of administrative and legal regulation of activities in the field of civil protection of the population and territories from emergencies. In particular, the development and implementation of the FEMA Federal Plan, which is the main act in the process of responding to an emergency and eliminating its consequences, should be included in the positive experience. Also positive is the experience of building the structure and organization of the activities of the Federal Emergency Management Agency (FEMA), in particular its functions in terms of administration and coordination of the activities of other public administration bodies in the specified area of public relations.

The feasibility of borrowing the structure and content of the official FEMA website, which contains detailed information for both government officials and citizens on the organization of civil protection of the population and territories of the United States from emergencies, is indicated. Attention is drawn to FEMA's experience in coordinating the activities of public administration bodies in terms of timely response to emergencies and prompt elimination of their negative consequences, as well as the accumulation of information about emergencies, which is provided by means of communication using the latest innovative information

technologies (high-speed fiber optic communication, secure server equipment, cloud technologies, the capabilities of social networks and messengers, artificial intelligence technology, etc.).

It is noted that the positive experience of the United States in developing and implementing a federal emergency response plan has been implemented into national legislation at the level of the Resolution of the Cabinet of Ministers of Ukraine dated March 14, 2018 № 223 «On Approval of the State-Level Emergency Response Plan», which allows national public administration bodies to respond promptly to emergencies.

The feasibility of borrowing a three-tier system of public management of emergency management and their consequences in the Japanese State is emphasized, in which the municipal level plays a key role, that is, the organization of civil defense forces and means at the level of local governments, which allows for the most prompt response to the onset of an emergency, as well as conducting systematic training and exercises with the population in the field of civil defense.

The stability of Japan's national legislation and the stability (traditionalism) of the functioning of public administration bodies that implement the state policy of the Japanese State in the field of ensuring fire safety are shown. This experience is worth borrowing by Ukraine, because constant reforms of central executive bodies, including public administration bodies that implement state policy in the field of civil protection, do not contribute to their effective work, which includes the formation of traditions, coherence and cohesion of collectives, internal subculture, etc.

The experience of the Japanese State in creating «municipal corporations» or «associations of districts» with the aim of consolidating financial and organizational resources for the elimination of emergency situations is called positive. Also positive is the experience of the functioning of volunteer fire brigades, which consist of volunteer firefighters who have their own employment or are employed in other paid work (however, in the event of a fire or other emergency, officials and other

members of volunteer fire brigades must follow the orders of the head of the fire department or fire station).

Attention is drawn to the Israeli national security doctrine, the effectiveness of which has been confirmed during the protection of the civilian population in conditions of ongoing military confrontation. For Ukraine, which is in a similar situation, the Israeli model of combining the forces and means of military command and civilian public administration bodies in organizing the elimination of emergencies and their consequences, including the use of modern information technologies in the field of ensuring the safety of life, namely the latest systems for notifying the civilian population about the threat of rocket attacks, is relevant. The military-oriented approach to crisis management in Israel deserves more detailed research and implementation into national legislation and legal practice.

The positive experience of the State of Israel in involving volunteer firefighters to eliminate emergencies was also highlighted.

According to the results of the study of current areas of improvement of administrative and legal regulation of the use of information technologies in the field of ensuring life safety, the following promising areas of normative activity in the specified area of public relations were identified:

- administrative and legal regulation of the development and functioning of a unified information and telecommunications system of civil protection, which will include, among other things, an interactive map of protective shelters (with the possibility of building a route for a person taking into account geolocation), places of localization of emergencies and their consequences (excluding places of arrival of enemy missiles and unmanned aerial vehicles), as well as an information base of subjects of ensuring civil protection and life safety;

- administrative and legal regulation of the development, distribution (popularization), as well as the procedure for administering and using a mobile application intended for the mobilization of human and material and technical resources in the event of a threat of an emergency or the immediate occurrence of an emergency, namely, approval by a joint order of the Ministry of Internal Affairs

of Ukraine and the Ministry of Digital Transformation of Ukraine of the procedure for using the Alert and Response System «I am a Volunteer» and the corresponding mobile application, which will contribute to the involvement of socially active citizens in the elimination of emergencies and their consequences;

- administrative and legal definition of the system of subjects of information technology use in the field of ensuring the safety of life, which will administer the unified information and telecommunications system of civil protection, as well as carry out operational maintenance (management of the control center) of mobile applications intended for the mobilization of human and material and technical resources in the event of a threat of an emergency or the immediate occurrence of an emergency;

- administrative and legal regulation of the issue of financial and logistical support for the functioning of the unified information and telecommunications system of civil protection, a mobile application for the mobilization of human and logistical resources in the event of a threat of or the immediate occurrence of an emergency, as well as the issue of financial and logistical support for entities that will be involved on a voluntary basis in the elimination of emergencies and their consequences;

- adoption of a separate Law of Ukraine «On Artificial Intelligence», which will regulate, among other things, the main issues of using artificial intelligence technology in the unified state system of civil protection and in the mechanism for ensuring the safety of life in general, as well as administrative and legal regulation of the procedure for using artificial intelligence technology in the field of ensuring the safety of life at the level of subordinate (departmental) regulatory legal acts;

- administrative and legal regulation of the storage of important information in the field of civil protection and ensuring the safety of life on several alternative servers, including servers located in foreign countries that have reliable partnership relations with Ukraine;

- administrative and legal regulation of the use of robotics, which is capable of replacing a person in the process of eliminating especially dangerous emergencies and their consequences;

- establishing administrative responsibility for failure to comply with the established procedure for conduct during an air alert in public places, at enterprises, institutions and organizations, regardless of their form of ownership, which requires amendments to the current Code of Ukraine on Administrative Offenses and approval of a prospective Procedure for Conduct in Public Places, at Enterprises, Institutions and Organizations, regardless of their form of ownership, during an air alert.

The above list is not exhaustive, because in the modern digitalized society, new information technologies appear almost every day, some of which can be used in the field of ensuring life safety and, accordingly, will require appropriate administrative and legal regulation.

Key words: administrative and legal principles, artificial intelligence, automated systems, civil protection, emergencies, information technologies, legal regulation, life safety, liquidation, mobile applications, prevention.

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Монографія:

1. Бондар Д.В. Адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності : монографія. Одеса: Видавництво «Юридика», 2025. 305 с.

Статті в періодичних фахових наукових виданнях України:

1. Бондар Д.В. Використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності: адміністративно-правові засади. *Право та державне управління*. 2024. № 3. С. 13–20. DOI: https://doi.org/10.32782/

pdu.2024.3.2.

2. Бондар Д.В. Заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій: адміністративно-правова регламентація та напрями удосконалення в умовах цифровізації. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 4. С. 46–54. DOI: https://doi.org/10.32782/2408-9257-2024-4-8.

3. Бондар Д.В. Історіографія та методологія дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал*. 2024. № 11. С. 270–274. DOI: https://doi.org/10.32782/2524-0374/2024-11/61.

4. Бондар Д.В. Актуальні напрями удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Juris Europensis Scientia*. 2024. № 6. С. 48–53. DOI: https://doi.org/10.32782/chern.v6.2024.9.

5. Бондар Д.В. Система принципів, напрямів та способів адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Київський часопис права*. 2024. № 4. С. 40–48. DOI: https://doi.org/10.32782/klj/2024.4.6.

6. Бондар Д.В. Адміністративно-правові засади використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності: сучасний стан та напрями удосконалення. *Право і суспільство*. 2024. № 6. С. 118–125. DOI: https://doi.org/10.32842/2078-3736/2024.6.18.

7. Бондар Д.В. Особливості понятійно-категоріального апарату та основні наукові підходи до дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний вісник*. 2024. № 6. С. 30–38. DOI: https://doi.org/10.32782/yuv.v6.2024.4.

8. Бондар Д.В. Досвід адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі. *Правові новели*. 2024. № 24. С. 68–76. DOI: https://doi.org/10.32782/ln.2024.24.10.

9. Бондар Д.В. Особливості адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в США. *Держава та регіони. Серія: Право*. 2024. № 4. С. 51–58. DOI: https://doi.org/10.32782/1813-338X-2024.4.7.

10. Бондар Д.В. Адміністративно-правові засади забезпечення безпеки життєдіяльності та цивільного захисту в Японській Державі в умовах цифровізації. *Право та державне управління*. 2024. № 4. С. 36–45. DOI: https://doi.org/10.32782/pdu.2024.4.5.

11. Бондар Д.В. Особливості адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану. *Науковий вісник Міжнародного гуманітарного університету. Серія: «Юриспруденція».* 2024. № 72. С. 30–35. DOI: https://doi.org/10.32782/2307-1745.2024.72.5.

12. Бондар Д.В. Безпека життєдіяльності в умовах інформаційного суспільства: актуальні питання та адміністративно-правові засоби їх вирішення. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 6. С. 90–97. DOI: https://doi.org/10.32782/2408-9257-2024-6-14.

13. Бондар Д.В. Забезпечення безпеки життєдіяльності та цивільний захист: співвідношення понять та особливості адміністративно-правового регулювання. *Науковий вісник публічного та приватного права*. 2024. № 6. С. 35–43. DOI: https://doi.org/10.32844/2618-1258.2024.6.6.

14. Бондар Д.В. Історія становлення та розвитку органів публічної адміністрації у сфері забезпечення безпеки життєдіяльності та цивільного захисту в контексті адміністративно-правового регулювання та цифровізації їх діяльності. *Правова позиція*. 2024. № 4(45). С. 82–89. DOI: https://doi.org/10.32782/2521-6473.2024-4.15.

15. Бондар Д.В. Реалізація публічних та приватних інтересів в процесі адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал*. 2024. № 10. С. 654–657. DOI: https://doi.org/10.32782/2524-0374/2024-10/156.

16. Бондар Д.В. Цифровізація систем цивільного захисту та забезпечення безпеки життєдіяльності: актуальні питання правового регулювання та матеріально-технічного забезпечення. *Юридичний науковий електронний журнал*. 2024. № 12. С. 543–546. DOI: https://doi.org/10.32782/2524-0374/2024-12/126.

17. Бондар Д.В. Адміністративно-правове регулювання захисту персональних даних та інформаційної безпеки у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал*. 2025. № 1. С. 601–605. DOI: https://doi.org/10.32782/2524-0374/2025-1/140.

18. Бондар Д.В. Адміністративно-правове регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності. *Право і суспільство*. 2024. № 5. С. 665–672. DOI: https://doi.org/10.32842/2078-3736/2024.5.96.

Статті в періодичних наукових виданнях,
які індексуються в наукометричних базах Web of Sciences та Scopus:

1. Бондар Д., Бакала В. Протипожежний напрям діяльності національно-культурних товариств на Східній Галичині в 1920–1930-х рр. *Skhidnoievropeiskyi istorychnyi visnyk – East European Historical Bulletin*. 2024. № 33. С. 139–148. DOI: https://doi.org/10.24919/2519-058X.33.317455.

2. Bondar D. Legal means of ensuring life safety in the context of the digitalization of public administration and the economy. *Baltic Journal of Economic Studies*. 2024. Vol. 10. № 4. P. 101–105. DOI: https://doi.org/10.30525/2256-0742/2024-10-4-101-105.

3. Bondar D.V. The system of entities using information technologies in the field of life safety: administrative, legal and economic principles of effective functioning. *Baltic Journal of Economic Studies*. 2024. Vol. 10. № 5. P. 131–136. DOI: https://doi.org/10.30525/2256-0742/2024-10-5-131-136.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Бондар Д.В. Актуальні напрями адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Теоретичні та практичні проблеми реалізації норм права* : X Міжнародна науково-практична конференція, м. Кременчук, 5–7 грудня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 199–203. DOI: https://doi.org/10.36059/978-966-397-452-1-52.

2. Бондар Д.В. Принципи адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Proceedings of the international scientific conference "Theoretical foundations of law, public management and practice of their application"*, Riga, the Republic of Latvia, December 25–26, 2024. Riga : Publishing House "Baltija Publishing", 2024. P. 83–88. DOI: https://doi.org/10.30525/978-9934-26-526-6-18.

3. Бондар Д.В. Адміністративно-правове регулювання використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності. *Становлення та розвиток правової держави: проблеми теорії та практики* : XVII Міжнародна науково-практична конференція, м. Миколаїв, 26 грудня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 93–95. DOI: https://doi.org/10.36059/978-966-397-463-7-23.

4. Бондар Д.В. Адміністративно-правова регламентація використання мобільного застосунку «Я – доброволець» з метою удосконалення систем забезпечення безпеки життєдіяльності та цивільного захисту в Україні. *Proceedings of the international scientific conference "The latest law developments"*, Wloclawek, Republic of Poland, April 3–4, 2024. Riga :

Publishing House “Baltija Publishing”, 2024. P. 308–311. DOI: https://doi.org/10.30525/978-9934-26-432-0-72.

5. Бондар Д.В. Актуальні питання правового регулювання та матеріально-технічного забезпечення використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Proceedings of the international scientific conference “Advances in law: the view of domestic and foreign scholars”*, Riga, the Republic of Latvia, October 3–4, 2024. Riga : Publishing House “Baltija Publishing”, 2024. P. 313–315. DOI: https://doi.org/10.30525/978-9934-26-493-1-80.

6. Бондар Д.В. Захист персональних даних у сфері забезпечення безпеки життєдіяльності: правове регулювання та європейські стандарти. *Proceedings of the international scientific conference “Scientific innovations in law amidst the impact of the Russian-Ukrainian war on the legal system”*, Riga, the Republic of Latvia, February 7–8, 2024. Riga : Publishing House “Baltija Publishing”, 2024. P. 316–319. DOI: https://doi.org/10.30525/978-9934-26-409-2-76.

7. Бондар Д.В. Адаптація національного законодавства у сферах цивільного захисту, використання інформаційних технологій та забезпечення безпеки життєдіяльності до права Європейського Союзу. *Юридичні науки: проблеми та перспективи* : матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 23–24 лютого 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 293–297. DOI: https://doi.org/10.36059/978-966-397-374-6-84.

8. Бондар Д.В. Трансформація національного законодавства у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах євроінтеграції та цифровізації. *Актуальні питання розвитку юридичної науки в період воєнного стану* : міжнародна науково-практична конференція, Науково-дослідний інститут публічного права, 17 травня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 363–367. DOI: https://doi.org/10.36059/978-966-397-395-1-107.

9. Бондар Д.В. Перспективні напрями удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері цивільного захисту та забезпечення безпеки життєдіяльності. *Теоретичні та практичні проблеми реалізації норм права* : матеріали IX Міжнародної науково-практичної конференції, м. Кременчук, 22–23 грудня 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 596–599. DOI: https://doi.org/10.36059/978-966-397-351-7-164.

10. Бондар Д.В. Адміністративно-правове регулювання використання інформаційних технологій у сфері цивільного захисту та забезпечення безпеки життєдіяльності в особливий період. *Восьмі Таврійські юридичні наукові читання* : матеріали міжнародної науково-практичної конференції, м. Київ, 16–17 червня 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 382–387. DOI: https://doi.org/10.36059/978-966-397-318-0-105.

ЗМІСТ

ВСТУП……34

РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ……..…….……48

1.1 Історіографія проблематики адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності……....48

1.2 Методологія дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності…….……66

1.3 Історія становлення та розвитку адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності……....88

Висновки до розділу 1……...105

РОЗДІЛ 2 СУЧАСНИЙ СТАН АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ…….…..…108

2.1 Адміністративно-правові засади побудови системи цивільного захисту та забезпечення безпеки життєдіяльності в Україні……..…..108

2.2 Заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій……..……..…147

2.3 Національна система суб’єктів забезпечення цивільного захисту та безпеки життєдіяльності…….……164

Висновки до розділу 2……..…….176

РОЗДІЛ 3 ЗАРУБІЖНИЙ ДОСВІД АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ В КОНТЕКСТІ ЦИФРОВІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ……..…….179

3.1 Адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в країнах-членах Європейського Союзу: позитивний досвід для України……179

3.2 Особливості адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в Сполучених Штатах Америки, Канаді та Сполученому Королівстві Великої Британії та Північної Ірландії……198

3.3 Адміністративно-правові засади забезпечення безпеки життєдіяльності та цивільного захисту в країнах Близького та Далекого Сходу в умовах цифровізації……..……217

Висновки до розділу 3……..….236

РОЗДІЛ 4 АКТУАЛЬНІ НАПРЯМИ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ В КОНТЕКСТІ ЦИФРОВІЗАЦІЇ……...……240

4.1 Адміністративно-правові засади цифровізації системи публічного управління в Україні……240

4.2 Правові засоби забезпечення безпеки життєдіяльності в контексті цифровізації публічного управління та економіки……...……281

4.3 Перспективні напрями удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту……301

Висновки до розділу 4……..….329

ВИСНОВКИ…….333

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……..…346

ДОДАТКИ……...…….395

ВСТУП

Актуальність теми дослідження. Питання забезпечення безпеки життєдіяльності у сучасному світі набувають усе більшої актуальності, адже розвиток високотехнологічного виробництва, поява технології штучного інтелекту та роботизованих систем вимагають 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 непоодинокими є випадки несанкціонованого втручання в роботу вказаних систем, що призводить до техногенних аварій та навіть катастроф. Крім того, досягнення науково-технічного прогресу часто умисно використовуються з протиправною метою або у військових цілях.

Водночас інноваційні інформаційні технології дозволяють значно удосконалити механізм публічного управління та адміністрування суспільних відносин. Електронний документообіг, надання адміністративних послуг у режимі онлайн, автоматизовані камери відеоспостереження, електронні державні реєстри та цифрові засоби комунікації значно оптимізують діяльність органів публічної адміністрації.

Вищевикладеним обґрунтовується необхідність належного правового врегулювання процесів цифровізації загалом та використання нових інформаційних технологій з метою забезпечення безпеки життєдіяльності зокрема. 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, а також удосконалення діяльності органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту.

Сучасний механізм забезпечення безпеки життєдіяльності та система цивільного захисту функціонують у складних умовах правового режиму воєнного стану, коли рятувальники, окрім виконання звичайних завдань, задіяні в ліквідації надзвичайних ситуацій воєнного характеру. Подвійне навантаження на Державну службу України з надзвичайних ситуацій зумовлює необхідність пошуку додаткових людських та матеріально-технічних ресурсів, які можна буде спрямувати на виконання завдань цивільного захисту, включаючи ліквідацію надзвичайних ситуацій та їх наслідків. Ключову роль у мобілізації вказаних додаткових ресурсів також можуть відігравати інноваційні інформаційні технології за умови належної адміністративно-правової регламентації. Належна правова регламентація забезпечить уніфікований підхід до використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту, що певною мірою гарантуватиме сумісність програмного забезпечення та централізований захист службової інформації, а також дозволить оперативно поширювати позитивний локальний досвід використання цифрових технологій у вказаній сфері суспільних відносин на територію всієї держави.

На окрему увагу заслуговує досвід зарубіжних країни у сфері публічного управління та адміністративно-правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. З урахуванням прагнення України набути повноправного членства в Європейському Союзі імплементації в національне законодавство потребують норми права ЄС, якими врегульовано питання використання технології штучного інтелекту та захисту персональних даних.

Вищезазначене зумовлює актуальність, а також теоретичну та практичну значимість дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Актуальні питання забезпечення безпеки життєдіяльності та цивільного захисту завжди перебували у центрі уваги науковців. Так, питанням

забезпечення безпеки життєдіяльності присвятили свої роботи такі відомі науковці, як Ф. Апшай, Т. Гринюк, К. Марченко, О. Оришака, О. Остапенко, О. Халак, О. Хитра, О. Чекригін та інші дослідники.

Питання адміністративно-правового регулювання суспільних відносин, включаючи суспільні відносини у сфері забезпечення безпеки життєдіяльності та цивільного захисту, досліджували такі відомі науковці, як: М. Бабик, В. Бевзенко, О. Берназюк, Д. Бєлов, Ю. Бисага, Д. Біленька, В. Доненко, О. Дубинський, К. Дубова, Т. Карабін, Т. Ковальова, Т. Коломоєць, О. Комаров, А. Комзюк, А. Краковська, Я. Лазур, І. Лопушинський, Р. Миронюк, А. Омельченко, І. Тищенкова та інші.

Правове регулювання використання та розвитку інформаційних технологій також є предметом дослідження багатьох науковців. Із останніх наукових праць, присвячених вказаній тематиці, слід виділити роботи В. Антонюка, О. Берназюка, Д. Біленької, О. Гунбіної, Т. Ковальової, О. Комарова, А. Краковської, Н. Литвин, І. Лопушинського, В. Любліна, А. Омельченка, М. Серебра, Р. Стефанчука, І. Тищенкової.

Проте питання адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності ще не були предметом окремого дослідження, що актуалізує необхідність цього дослідження з метою формулювання пропозицій щодо вдосконалення чинного адміністративного законодавства та юридичної практики у зазначеній сфері суспільних відносин.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертація виконана відповідно до Стратегії розвитку Національної академії правових наук України на 2021–2025 рр.; Закону України «Про Національну програму інформатизації» від 1 грудня 2022 р. № 2807-IX; Указу Президента України від 30 вересня 2019 р. № 722 «Про цілі сталого розвитку України на період до 2030 року»; Стратегії національної безпеки України, затвердженої указом Президента України від 14 вересня 2020 р. № 392; Державної стратегії регіонального розвитку на 2021–2027 рр.,

затвердженої постановою Кабінету Міністрів України від 5 серпня 2020 р. № 695; Засад реалізації органами виконавчої влади принципів державної політики цифрового розвитку, затверджених постановою Кабінету Міністрів України від 30 січня 2019 р. № 56; Стратегії розвитку сфери інноваційної діяльності на період до 2030 р., схваленої розпорядженням Кабінету Міністрів України від 10 липня 2019 р. № 526-р; Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р.

Мета дослідження. Мета дисертаційної роботи полягає в тому, щоб на основі комплексного аналізу теоретичних напрацювань, положень чинного законодавства України та практики його застосування визначити правову природу і сутність адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності; окреслити тенденції та виявити недоліки категоріального, нормативного, інституційного й інструментального складників адміністративно-правового регулювання використання інформаційних технологій у вказаній сфері суспільних відносин; сформулювати науково обґрунтовані висновки, теоретичні положення та практичні рекомендації, спрямовані на підвищення результативності й ефективності адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Для досягнення цієї мети в роботі необхідно послідовно вирішити такі основні *задачі*:

– охарактеризувати історіографію проблематики адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності;

– визначити методологію дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності;

– охарактеризувати історію становлення та розвитку адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності;

– систематизувати адміністративно-правові засади побудови системи цивільного захисту та забезпечення безпеки життєдіяльності в Україні;

– узагальнити заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій;

– охарактеризувати національну систему суб'єктів забезпечення цивільного захисту та безпеки життєдіяльності;

– визначити особливості адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в країнах-членах Європейського Союзу;

– охарактеризувати особливості правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту у Сполучених Штатах Америки та Сполученому Королівстві Великої Британії та Північної Ірландії;

– узагальнити адміністративно-правові засади забезпечення безпеки життєдіяльності та цивільного захисту в країнах Близького та Далекого Сходу в умовах цифровізації;

– охарактеризувати адміністративно-правові засади цифровізації системи публічного управління в Україні;

– систематизувати правові засоби забезпечення безпеки життєдіяльності в контексті цифровізації публічного управління та економіки;

– визначити перспективні напрями удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту.

Об'єктом дослідження є врегульовані нормами адміністративного права суспільні відносини у сфері забезпечення безпеки життєдіяльності та цивільного захисту.

Предметом дослідження є адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності

Методи дослідження. У ході дисертаційного дослідження використано класичну систему філософських, загальнонаукових та спеціально-юридичних методів дослідження, а також інструментальний, історико-правовий, телеологічний, антропоцентричний, цивілізаційний та синергетичний наукові підходи, які дали змогу дослідити адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та визначити перспективні напрями удосконалення національного законодавства у цій сфері суспільних відносин.

Так, для дослідження історіографії проблематики адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності використано прийоми логічного методу, системний і структурно-функціональний методи, а також історико-правовий та цивілізаційний наукові підходи (підрозділ 1.1). З метою визначення методології дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності використано закони та прийоми діалектики, системний метод і прийоми логічного методу (підрозділ 1.2). Для аналізу історії становлення та розвитку адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності використано історико-правовий підхід та прийоми логіки, а також закони діалектики та системний метод (підрозділ 1.3).

З метою дослідження адміністративно-правових засад побудови системи цивільного захисту та забезпечення безпеки життєдіяльності в Україні використано закони та прийоми діалектики, прийоми логічного методу, системний та структурно-функціональний методи, інструментальний та цивілізаційний підходи (підрозділ 2.1). Для аналізу заходів забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій використано прийоми логіки, системний і структурно-функціональний

методи, інструментальний та синергетичний наукові підходи, а також метод статистики (підрозділ 2.2). Для характеристики національної системи суб'єктів забезпечення цивільного захисту та безпеки життєдіяльності використано структурно-функціональний та системний методи, формально-юридичний метод, антропоцентричний та телеологічний наукові підходи (підрозділ 2.3).

З метою визначення особливостей адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в країнах-членах Європейського Союзу використано системний метод, прийоми логічного методу, формально-юридичний метод та методологію порівняльного правознавства (підрозділ 3.1). Для характеристики особливостей адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту у Сполучених Штатах Америки та Сполученому Королівстві Великої Британії та Північної Ірландії використано методологію порівняльного правознавства, системний і структурно-функціональний методи, а також цивілізаційний науковий підхід (підрозділ 3.2). Для визначення особливостей адміністративно-правових засад забезпечення безпеки життєдіяльності та цивільного захисту в країнах Близького та Далекого Сходу в умовах цифровізації використано прийоми логічного методу, системний метод, методологію порівняльного правознавства та цивілізаційний науковий підхід (підрозділ 3.3).

З метою характеристики адміністративно-правових засад цифровізації системи публічного управління в Україні використано системний та формально-юридичний методи, синергетичний та інструментальний наукові підходи (підрозділ 4.1). Для систематизації правових засобів забезпечення безпеки життєдіяльності в контексті цифровізації публічного управління та економіки використано закони та прийоми діалектики, прийоми логічного методу, системний і структурно-функціональний методи, антропоцентричний та інструментальний наукові підходи (підрозділ 4.2). Для визначення перспективних напрямів удосконалення адміністративно-правового

регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту використано прийоми логічного методу, формально-юридичний метод, метод юридичного моделювання, антропоцентричний, інструментальний та синергетичний наукові підходи (підрозділ 4.3).

Нормативну основу роботи становлять Конституція України, міжнародні нормативно-правові акти (конвенції, угоди) у сфері цифровізації, забезпечення безпеки життєдіяльності та цивільного захисту, ратифіковані Верховною Радою України, кодекси та закони України, укази Президента України, постанови Кабінету Міністрів України, правові позиції (висновки) Верховного Суду, підзаконні (відомчі) нормативно-правові акти центральних органів виконавчої влади, зокрема накази Міністерства внутрішніх справ України, Державної служби України з надзвичайних ситуацій та Міністерства цифрової трансформації України, спільні накази органів публічної адміністрації та акти органів місцевого самоврядування.

Емпіричною базою дисертації є дані, акумульовані Міністерством внутрішніх справ України, Міністерством цифрової трансформації України, Державною службою України з надзвичайних ситуацій та Державною службою статистики України, а також правова публіцистика, довідкові та енциклопедичні видання, матеріали актуальних і репрезентативних соціологічних досліджень тощо.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших у юридичній науці комплексних досліджень адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, у якому не лише розкрито особливості адміністративно-правового регулювання у вказаній сфері суспільних відносин, а й наведено ґрунтовний аналіз теоретичних і методологічних засад побудови та функціонування механізму забезпечення безпеки життєдіяльності в Україні в умовах євроінтеграції та цифровізації з урахуванням позитивного зарубіжного досвіду й міжнародних стандартів.

Унаслідок здійсненого дослідження сформульовано низку положень і висновків, запропонованих особисто здобувачем, зокрема:

уперше:

– сформульовано авторське визначення безпеки життєдіяльності в контексті цифровізації як комплексної науки та навчальної дисципліни, яка досліджує всі негативні чинники (небезпеки), які впливають або потенційно можуть вплинути на життєдіяльність людини у сучасному інформаційному суспільстві, порушити порядок нормального функціонування та розвитку суспільства загалом, встановлює систему технічних та техніко-юридичних норм взаємодії людини із навколишнім середовищем та цифровим світом, а також визначає систему засобів запобігання та протидії вказаним негативним чинникам (небезпекам), ліквідації надзвичайних ситуацій та їх наслідків, включаючи інноваційні інформаційні технології, використання яких потребує належної адміністративно-правової регламентації;

– встановлено, що адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволяє уніфікувати, стандартизувати програмне забезпечення, яке використовується різними органами публічної адміністрації (що гарантує сумісність цифрових технологій у процесі їх використання), забезпечити централізований захист інформаційних ресурсів у сфері забезпечення безпеки життєдіяльності та цивільного захисту, а також поширити локальний позитивний досвід використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності на територію всієї держави;

– запропоновано класифікувати інформаційні технології, які використовуються у сфері забезпечення безпеки життєдіяльності та потребують детальної адміністративно-правової регламентації, на: автоматизовані інформаційні системи, автоматизовані (роботизовані) системи ліквідації надзвичайних ситуацій та їх наслідків, мобільні застосунки та

месенджери соціальних мереж, а також інструменти (алгоритми) технології штучного інтелекту;

– обґрунтовано необхідність розробки та прийняття спільного наказу Міністерства внутрішніх справ України та Міністерства цифрової трансформації України, яким буде затверджено порядок функціонування та використання Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку, що дозволить створити інформаційну базу фізичних осіб-добровольців з урахуванням їхньої фахової підготовки та спеціалізації, місця проживання або місцезнаходження (геолокації) та оперативно мобілізувати людські і матеріально-технічні ресурси для ліквідації надзвичайних ситуацій та їх наслідків;

– запропоновано розробити та прийняти Закон України «Про використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності» (як варіант доповнити Розділ ІІ Кодексу цивільного захисту України новою главою «Використання технології штучного інтелекту в єдиній державній системі цивільного захисту»), яким буде врегульовано, зокрема, використання технології штучного інтелекту в єдиній державній системі цивільного захисту та в механізмі забезпечення безпеки життєдіяльності загалом;

удосконалено:

– методологічні засади дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які запропоновано доповнити такими науковими підходами, як інструментальний, цивілізаційний, телеологічний, антропологічний та синергетичний, що дасть змогу врахувати всі об’єктивні і суб’єктивні чинники, які впливають на особливості використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та зумовлюють необхідність адміністративно-правової регламентації їх використання;

– наукові підходи до розуміння системи суб'єктів забезпечення безпеки життєдіяльності та цивільного захисту, ключовим засобом удосконалення діяльності яких названо подальшу автоматизацію та інформатизацію (цифровізацію) у процесі забезпечення безпеки життєдіяльності загалом та цивільного захисту зокрема шляхом упровадження автоматизованих корпоративних інформаційних систем, автоматизованих систем ліквідації надзвичайних ситуацій, мобільних застосунків для оповіщення населення про загрозу чи настання надзвичайної ситуації та мобілізації людських і матеріально-технічних ресурсів, використання технології штучного інтелекту;

– положення про систему адміністративно-правових засобів забезпечення безпеки життєдіяльності та цивільного захисту в умовах євроінтеграції та цифровізації, а саме обґрунтування необхідності використання спільної нормотворчої діяльності МВС України, ДСНС України та Міністерства цифрової трансформації України з метою забезпечення своєчасного та якісного адміністративно-правового врегулювання використання інноваційних інформаційних технологій у сфері забезпечення безпеки життєдіяльності;

набули подальшого розвитку:

– узагальнення досвіду теоретико-методологічного та адміністративно-правового забезпечення безпеки життєдіяльності в зарубіжних країнах (включаючи правове регулювання використання інформаційних технологій), серед яких особливу увагу приділено позитивному досвіду Сполучених Штатів Америки, Канади, Сполученого Королівства Великої Британії та Північної Ірландії, Держави Ізраїль, Японської Держави, Китайської Народної Республіки та країн Європейського Союзу, оскільки системи забезпечення безпеки життєдіяльності в них демонструють високий рівень організації (включаючи адміністративно-правове забезпечення), автоматизації (цифровізації) та відповідності світовим стандартам;

– систематизація історіографії дослідження проблематики адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту з метою впорядкування доктринальної основи для формулювання конкретних науково обґрунтованих пропозицій щодо вдосконалення чинного адміністративного законодавства, а також національного законодавства у сфері інформатизації (цифровізації) та забезпечення безпеки життєдіяльності;

– науково обґрунтовані положення щодо необхідності встановлення адміністративної відповідальності за невиконання встановленого порядку поведінки під час оголошення повітряної тривоги в публічних місцях, на підприємствах, установах та організаціях, незалежно від форми власності, що потребує внесення змін до чинного Кодексу України про адміністративні правопорушення та затвердження перспективного Порядку поведінки в публічних місцях, на підприємствах, установах та організаціях, незалежно від форми власності, під час повітряної тривоги.

Практичне значення отриманих результатів полягає в тому, що сформульовані в дисертаційному дослідженні доктринальні положення, узагальнення, науково обґрунтовані висновки та пропозиції мають загальнотеоретичне й прикладне значення для доктрини адміністративного права, законотворчої і нормотворчої діяльності та юридичної практики у сфері забезпечення безпеки життєдіяльності та цивільного захисту. Результати дослідження можуть бути використані в таких напрямах:

– *науково-дослідній сфері* – для розроблення актуальних напрямів удосконалення теоретико-методологічних і правових засад функціонування механізму забезпечення безпеки життєдіяльності та цивільного захисту в умовах цифровізації публічного управління та економіки, а також для вивчення відповідних правових механізмів на загальнотеоретичному рівні й у межах інших галузей права;

– *правотворчій діяльності* – для розроблення пропозицій щодо внесення змін до Кодексу цивільного захисту України, Кодексу України про адміністративні правопорушення, а також розроблення та прийняття спільного наказу МВС України та Міністерства цифрової трансформації України про затвердження Порядку функціонування і використання Системи реагування та оповіщення «Я – доброволець» та відповідного мобільного застосунку;

– *правозастосовній діяльності* – для поліпшення й удосконалення практики використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту населення і територій від надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру;

– *навчальному процесі* – для підготовки підручників, посібників та інших навчально-методичних матеріалів зі спеціальностей «Адміністративне право», «Інформаційне право», «Безпека життєдіяльності», а також під час викладання відповідних дисциплін.

Особистий внесок здобувача. Основні положення й висновки дисертації розроблено автором самостійно з використанням новітніх досягнень вітчизняної науки адміністративного права та робіт зарубіжних учених-адміністративістів. Усі положення й висновки, викладені в дисертації, ґрунтуються на власних дослідженнях автора. За результатами дослідження опубліковано монографію «Адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності» (2025 р.).

Апробація матеріалів дисертації. Основні теоретичні положення, висновки та пропозиції, що містяться в роботі, оприлюднені на 10 науково-практичних конференціях, зокрема: «Теоретичні та практичні проблеми реалізації норм права» (м. Кременчук, 5–7 грудня 2024 р.); «Theoretical foundations of law, public management and practice of their application» (м. Рига, Латвійська Республіка, 25–26 грудня 2024 р.); «Становлення та розвиток

правової держави: проблеми теорії та практики» (м. Миколаїв, 26 грудня 2024 р.); «The latest law developments» (м. Влоцлавек, Республіка Польща, 3–4 квітня 2024 р.); «Advances in law: the view of domestic and foreign scholars» (м. Рига, Латвійська Республіка, 3–4 жовтня 2024 р.); «Scientific innovations in law amidst the impact of the Russian-Ukrainian war on the legal system» (м. Рига, Латвійська Республіка, 7–8 лютого 2024 р.); «Юридичні науки: проблеми та перспективи» (м. Запоріжжя, 23–24 лютого 2024 р.); «Актуальні питання розвитку юридичної науки в період воєнного стану» (Науково-дослідний інститут публічного права, 17 травня 2024 р.); «Теоретичні та практичні проблеми реалізації норм права» (м. Кременчук, 22–23 грудня 2023 р.); «Восьмі Таврійські юридичні наукові читання» (м. Київ, 16–17 червня 2023 р.).

Публікації. Основні положення роботи знайшли відображення в 1 одноосібній монографії, 21 науковій статті, з яких 3 статті опубліковані в наукових зарубіжних виданнях, що включені до наукометричних баз Scopus і Web of Science, та 18 статей – у періодичних виданнях України, що визнані як фахові з юридичних дисциплін, а також у 10 тезах доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, що містять дванадцять підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 403 сторінки, у тому числі основного тексту – 312 сторінок. Список використаних джерел налічує 368 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

1.1 Історіографія проблематики адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності

Будь-яке змістовне та всебічне дослідження актуальних питань адміністративно-правового регулювання суспільних відносин передбачає дослідження ступеня наукової розробки об’єкта та предмета наукового аналізу, адже сучасна доктрина адміністративного права сформувалась завдяки працям видатних вчених-адміністративістів, які присвятили свої роботи різним аспектам правового регулювання суспільних відносин. Аналіз історіографії дозволяє виявити ті проблемні питання, які потребують додаткового дослідження з метою формулювання конкретних пропозицій щодо удосконалення чинного адміністративного законодавства та юридичної практики.

Враховуючи тему даного дослідження, на увагу заслуговують не тільки наукові праці вчених-адміністративістів, але й дослідження науковців, присвячені використанню інноваційних інформаційних технологій з метою удосконалення суспільних відносин, включаючи сферу забезпечення безпеки життєдіяльності, а також наукові праці, присвячені актуальним питанням реформування інформаційного законодавства (правовим засадам використання інформаційних технологій) та питанням безпеки життєдіяльності і цивільного захисту.

Історіографія дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності об’єднує чотири групи наукових літературних джерел.

Перша група – підручники, навчальні посібники, монографії, публікації у періодичних виданнях, присвячені питанням забезпечення безпеки життєдіяльності, підготовлені фахівцями з прикладних, технічних та природничих наук. У вказаних наукових роботах розкривається сутність та складові безпеки життєдіяльності як науки та навчальної дисципліни, описуються основні заходи, способи та прийоми забезпечення безпеки життєдіяльності.

З останніх досліджень у вказаній сфері варто відзначити наукові публікації Л. Воловик, К. Ковальської та Р. Бондаренка «Безпека життєдіяльності населення в умовах глобалізації» [66], А. Вороніна «Сучасні проблеми безпеки життєдіяльності» [69], М. Завадської та Є. Осипенка «Забезпечення безпеки життєдіяльності людини в умовах екстремальних ситуацій» [109], Л. Калашнікової «Безпека життєдіяльності як предмет соціологічного аналізу: уточнення змісту поняття» [126], А. Качинського «Безпека життєдіяльності особи, суспільства та держави: порогові умови» [130], А. Полежаєва, С. Ковжоги, Є. Карманного та О. Малька «Особливості системи «Безпека життєдіяльності людини» як об’єкта управління» [219].

Так, Л. Воловик, К. Ковальська та Р. Бондаренко зазначають, що процес сталого розвитку людства тісно пов’язаний з питанням безпеки життя і здоров’я людини. В сучасний період ця проблема постає надзвичайно гостро. Вона є однією із пріоритетних у діяльності світової спільноти в умовах глобалізації в усіх сферах життєдіяльності населення: матеріально-виробничої, побутової, соціально-політичної та культурно-духовної. Незважаючи на різний рівень соціально-економічного розвитку країн, якість життя населення, глобальні проблеми людства торкаються всіх без виключення держав світу [66, с. 34].

Також науковці справедливо зазначають, що безпечна життєдіяльність населення неможлива без підготовки людини до активної участі у забезпеченні тривалого повноцінного життя в суспільстві, що динамічно змінюється. Успіх цього задуму можливий лише за умови усвідомлення

кожною людиною, що безпека її власного життя і безпека всього людства полягає у формуванні чітких світоглядних засад. Бо від знань людини, її ефективних дій, правильності рішень, моральних принципів залежить, чи вдасться вберегти життя на Землі. Саме розвиток усіх ланок освіти з питань безпеки людини надасть кожній людині можливість зрозуміти важливість свого гармонійного існування в навколишньому середовищі, а також навчить приймати правильні рішення в умовах виникнення різного роду небезпек [66, с. 36].

Варто погодитись із вищезазначеною позицією науковців, особливо в частині необхідності розвитку усіх ланок освіти з питань забезпечення безпеки життєдіяльності та цивільного захисту. Водночас слід наголосити на необхідності цифровізації діяльності органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, адже саме інформаційні технології здатні забезпечити ефективне централізоване публічне управління процесами попередження і ліквідації надзвичайних ситуацій та їх наслідків, а також уможливити всеохоплююче та систематичне навчання громадян засадам цивільного захисту та безпеки життєдіяльності (завдяки використанню технологій Інтернет, мобільних застосунків тощо).

А. Воронін слушно зауважує, що безпека людини – це поняття, що впливає на характер життя людини та сферу її діяльності. Це баланс між людьми, суспільством і країною. Важливість безпеки людини дає змогу розширити психологічне поле самозахисту особистості, зокрема розвинути її здатність піклуватися про себе, задовольняти свої потреби. Активна участь кожного громадянина в охороні довкілля та власному захисті є запорукою безпеки особистості, суспільства та людей на шляху до сталого розвитку та є важливою складовою суспільного та культурного життя. Тому свобода та захист є основними компонентами безпеки людського життя та діяльності, без яких неможливий збалансований людський розвиток. У сучасних умовах, коли розвиток світового господарства перетворив навколишнє середовище в єдиний інтегрований ресурс для використання та перетворення суспільними

виробничими системами, необхідно ретельно враховувати економічні фактори при розробці екологічного та соціального плану розвитку суспільства з метою забезпечення безпеки людини [69, с. 66].

Такий підхід заслуговує на увагу, проте А. Воронін дещо переоцінює роль економічних факторів в механізмі забезпечення безпеки життєдіяльності, а також перебільшує значення власного захисту (самозахисту) людини від негативних факторів навколишнього середовища. Ключову роль в організації ефективного та стабільного функціонування механізму забезпечення безпеки життєдіяльності та єдиної державної системи цивільного захисту повинні відігравати органи публічної адміністрації та конкретні суб'єкти владних повноважень зокрема, адже специфіка сучасного технологічно-розвинутого інформаційного суспільства полягає в проведенні масштабних загальнонаціональних реформ системи цивільного захисту, а також створенні безпечного життєвого простору для кожної людини з використанням стандартизованих високотехнологічних засобів. Наприклад, питання радіаційної безпеки знаходиться у сфері компетенції уповноважених органів публічної адміністрації і не залежать від поведінки окремих осіб, які не задіяні у відповідній галузі. Людина може забезпечити себе засобами індивідуального захисту, проте не може впливати на рівень захисту атомних електростанцій, або зупинити поширення радіації у випадку техногенної катастрофи. Навіть в питаннях організації протипожежного захисту промислових підприємств, об'єктів критичної інфраструктури все більшу роль відіграють інноваційні засоби контролю, які застосовують відповідні органи публічної адміністрації, а саме, стандартизовані автоматизовані системи протипожежної сигналізації, автоматизовані системи пожежогасіння тощо [212].

А. Полежаєв, С. Ковжога, Є. Карманний та О. Малько також слушно зазначають, що в сучасному світі питання безпеки життєдіяльності людини все більш постають на перший план. Це обумовлено зростанням та ускладненням техносфери, зростаючим негативним впливом людини на навколишнє середовище, а також зростанням вартості помилок та прорахунків людини при

здійсненні перетворюючої діяльності. Така динаміка рівня безпеки життєдіяльності викликає необхідність управляючого впливу – створення загальнодержавної системи управління безпекою життєдіяльності. Метою управління безпекою життєдіяльності людини є підтримання за рахунок управління потрібного рівня всебічної безпеки людини (суспільства). Водночас створення загальнодержавної системи управління безпекою життєдіяльності людини не можливе без розгляду особливостей об'єкта управління [219, с. 245].

Таким чином, науковці наголошують на тому, що в сучасному технологічному суспільстві питання безпеки життєдіяльності виходять на перший план та потребують особливої уваги з боку органів публічної адміністрації, інститутів громадянського суспільства та кожної окремої людини. Водночас створити ефективну загальнодержавну систему управління безпекою життєдіяльності неможливо без використання сучасних інноваційних інформаційних технологій, адже публічне управління в інформаційному суспільстві спирається на потужний та розгалужений цифровий інструментарій засобів впливу на суспільні відносини, донесення інформації до суб'єктів, засобів обробки та систематизації інформації, а також автоматизованих засобів реагування на відповідні ситуації.

Друга група наукових літературних джерел в історіографії дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності – це наукові видання, монографії, дисертаційні дослідження, присвячені питанням використання інформаційних технологій у різних сферах суспільних відносин, включаючи основні напрями та способи цифровізації, перехід на електронний документообіг в діяльності органів публічної адміністрації, використання цифрових інструментів для досягнення публічних та приватних цілей учасників суспільних відносин, надання цифрових послуг тощо. Це роботи фахівців у сфері інформатики та інформатизації, комп'ютерних наук, а також вчених-юристів, які досліджують питання використання інформаційних

технологій у сфері публічного управління.

З останніх досліджень на даному напрямі слід відзначити підручник В. Плескача та Т. Затонацької «Інформаційні системи і технології на підприємствах» [213], дисертаційне дослідження О. Берназюка «Цифрові технології у праві: тенденції та перспективи розвитку» та його монографію «Цифрові технології у праві: сучасний погляд у майбутнє» [27, 28], публікації С. Боліли «Роль інформаційних технологій та цифрових інструментів в умовах викликів війни та післявоєнного відновлення економіки України» [36], А. Краковської та М. Бабика «Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку» [154], Р. Стефанчука «Інформаційні технології та право: quo vadis?» [305].

Так, в підручнику «Інформаційні системи і технології на підприємствах», підготовленим В. Плескачем та Т. Затонацькою, підкреслено, що розвиток інформаційного суспільства в Україні і впровадження інформаційних технологій та інформаційних систем в усі сфери суспільного життя, а також в діяльність органів публічної адміністрації визначається одним із пріоритетних напрямів державної політики. А інформаційно-комунікаційна технологія визначається як система методів, процесів та способів використання обчислювальної техніки і систем зв’язку для створення, збирання, передавання, пошуку, обробки та поширення інформації з метою ефективної організації діяльності людей [213, с. 14].

Отже, основною метою впровадження інформаційних технологій в усі сфери суспільного життя є ефективна організація діяльності людей, включаючи відносини публічного управління та адміністрування суспільних відносин, а також сферу забезпечення безпеки життєдіяльності та цивільного захисту. Наведене визначення інформаційних технологій цілком відображає їх сутність, проте слід зазначити, що в сучасному інформаційному суспільстві ключову роль, наряду з засобами обчислювальної (комп’ютерної) техніки і системами зв’язку, відіграють програмні продукти – тобто програмне забезпечення для вирішення різноманітних задач. Саме комп’ютерні програми

як складні алгоритми обробки інформації дозволяють значно удосконалити, автоматизувати сучасні технологічні процеси, зокрема і в сфері забезпечення безпеки життєдіяльності.

О. Берназюк зазначає, що стрімкий розвиток науки та техніки обумовив перехід від індустріального до інформаційного суспільства, внаслідок чого постало питання про масштабне запровадження та використання цифрових технологій не тільки в повсякденному житті, виробничій та комерційній діяльності суб'єктів господарювання, але й у діяльності суб'єктів владних повноважень. З огляду на це в багатьох розвинутих країнах світу відбувся перехід до нової моделі публічного управління, заснованої на електронному урядуванні. Беручи до уваги світові тенденції у сфері розвитку та застосування цифрових технологій у праві, перед Україною постало завдання щодо подальшої їх інтеграції в різні сфери суспільного та державного життя з тим, щоб відповідати очікуванням та потребам інформаційного суспільства, вимогам європейських стандартів у сфері публічного управління [28, с. 3].

Отже, використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності є одним із напрямів загальної цифровізації публічного управління, розвитку електронного урядування, покликаного спростити (полегшити) життя людей та удосконалити їх відносини з органами публічної адміністрації. Крім того, для України цифровізація – це не тільки спосіб удосконалення існуючих суспільних відносин, включаючи відносини публічного управління, але й умова успішності євроінтеграційних процесів завдяки впровадженню європейських стандартів у сфері публічного управління та адаптації національного інформаційного законодавства до права ЄС.

С. Боліла за результатами дослідження ролі інформаційних технологій та цифрових інструментів в умовах викликів війни та післявоєнного відновлення економіки України, формулює важливий висновок про те, що системне запровадження сучасних інформаційних технологій та цифрових інструментів за для досягнення ефекту синергії в діяльність держави, бізнесу

та суспільства забезпечить оптимізацію цифрових процесів та буде сприяти реалізації пріоритетних інноваційних проєктів, важливих для відновлення та відбудови країни. Інноваційні інструменти діджиталізації світового рівня створять можливості для швидкої цифрової трансформації ключових галузей і сфер суспільного життя, розвитку цифрової економіки та ІТ-індустрії; підтримки формування української стартап-екосистеми, що зумовить невідворотність прогресивних соціально-економічних перетворень, дозволить зберегти стійкість економіки під час війни та її зростання після перемоги й зробить конкурентним та інвестиційно привабливим український бізнес.

На думку С. Боліли, інформаційні технології та цифрові моделі допоможуть країні, армії та бізнесу шляхом консолідації зусиль вистояти та протидіяти збройній агресії ворога та відновитися підприємствам не лише великого, а й середнього та малого бізнесу як на національному, так і на регіональному та локальному рівні, включаючи як промислові об’єкти, військово-оборонний комплекс, так і аграрну, туристичну, комерційну, сферу, ІТ-сектор, креативні індустрії та інші галузі економіки; забезпечать підвищення рівня інноваційності бізнес-структур, що буде чинником залучення інвестицій в розвиток їх діяльності та буде сприяти підвищенню їх конкурентоспроможності та прибутковості й дозволить створити робочі місця, що буде стимулом для повернення українців додому, сприятиме економічному відновленню та відбудові нашої країни та надасть можливість в найближчій перспективі зайняти гідне місце в європейській спільноті [36, с. 272].

Отже, використання інформаційних технологій все більшою кількістю учасників суспільних відносин матиме синергетичний ефект та призведе до переходу від кількісних змін до якісних, а саме, реального покращення життя людей, надійного та якісного забезпечення безпеки їх життєдіяльності та ефективного функціонування єдиної державної системи цивільного захисту в умовах повномасштабної війни російської федерації проти України. Головним в цьому процесі є поєднання зусиль органів публічної адміністрації та приватних компаній, бізнес-структур, які є більш гнучкими та

ініціативними у сфері впровадження та використання інформаційних технологій.

На думку А. Краковської та М. Бабика, сьогодні уявити наше життя без інформаційних технологій просто неможливо. Велика кількість сучасних потреб людини може бути задоволена завдяки стрімкому розвитку цифровізації. Потреби у сфері публічного адміністрування не є винятком. Наша країна обрала курс на формування «сервісної держави», що має на меті розробку великої кількості спеціальних додатків, ресурсів та програм, які мають на меті полегшити процеси отримання адміністративних послуг, що створює лише позитивний ефект на імідж держави як в очах її громадян, так і на світовій арені. Причиною такому процесу є низка факторів, серед яких: зручність отримання послуг в режимі онлайн, економія часу та енергії. Проявом цифровізації адміністративних послуг є запровадження процесу електронного урядування, необхідність та актуальність якого не викликає жодного сумніву, адже це вимога часу, наступний крок у розвитку суспільних відносин [154, с. 330].

Також А. Краковська та М. Бабик зазначають, що Україна має всі можливості для побудови ефективної системи цифровізованих адміністративних послуг, адже зроблено вже багато кроків, покликаних на ефективне функціонування даного процесу. Проте, як і з будь-яким новим процесом, який імплементується в суспільні відносини, виникають певні проблеми в його реалізації. І лише за умови системного підходу до вирішення цих проблем вдасться забезпечити якісний рівень функціонування системи електронних адміністративних послуг, як одного з важливих чинників розвитку демократії в країні та підвищення якості життя громадян нашої держави [154, с. 334].

Таким чином, цифровізація покликана суттєво удосконалити механізми публічного управління, забезпечити ефективне використання інформаційних технологій у всіх сферах суспільних відносин, що можливо за умови належного адміністративно-правового регулювання інформаційних відносин,

включаючи заходи адміністративної відповідальності за порушення встановленого порядку використання цифрових інструментів, а також використання останніх із протиправною метою.

Р. Стефанчук слушно зауважує, що розвиток ІТ, подальша інтеграція Інтернету в суспільне життя є неминучими процесами, що не залежатимуть від бажань держави. Питання полягатиме в готовності права запропонувати цим змінам сучасний, системний і адекватний підхід для того, щоб забезпечити належне регулювання цієї сфери з метою використання її на благо суспільства загалом та окремих осіб зокрема. Сьогодні, на думку Р. Стефанчука, перспективним убачається формування правової політики, спрямованої на процеси цифровізації людини й суспільних відносин. Основою такого процесу могла б стати технологія блокчейну, застосування якої сприятиме забезпеченню прозорості, ефективності, пришвидшенню процесів у більшості сфер людської життєдіяльності. Водночас доцільно подумати і про механізм протидії можливим негативним наслідкам від тотальної цифровізації життя людини [305, с. 44].

Таким чином, науковці в своїх дослідженнях приходять до висновків про неминучість процесів цифровізації суспільного життя та особливу роль інформаційних технологій в розвитку фактично всіх сфер суспільних відносин. Водночас дослідники застерігають про можливі негативні наслідки тотальної цифровізації, які становлять пряму або опосередковану загрозу безпеці життєдіяльності людини та суспільства в цілому, та, відповідно, потребують особливої уваги з боку органів публічної адміністрації.

Третя група – це дослідження, присвячені правовому регулюванню інформаційних відносин, включаючи адміністративно-правові засади інформатизації, використання цифрових інструментів, надання цифрових адміністративних послуг, а також правове регулювання порядку збирання, зберігання та використання інформації в комп’ютерних мережах, питання відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-

комунікаційних систем, електронних комунікаційних мереж, правове регулювання Інтернет, технології штучного інтелекту та інших інформаційних технологій. Вказані дослідження здійснюються вже вченими-юристами, включаючи фахівців у галузі адміністративного права і процесу, інформаційного права тощо.

Це, зокрема, дослідження Д. Біленської «Адміністративно-правове регулювання інформаційних відносин в Україні» [31], С. Єсімова «Використання інформаційних технологій як предмет адміністративно-правового регулювання» [107], Н. Коминара «Інформаційна безпека як складова національної безпеки держави: адміністративно-правовий аспект» [147], О. Кузьменко, В. Чорної та С. Островського «Правове регулювання запровадження та використання штучного інтелекту» [157], О. Олійника «Організаційно-правові засади захисту інформаційних ресурсів України» [190], А. Омельченка «Суспільні відносини у сфері цифровізації як предмет правового регулювання» [191].

Так, Д. Біленська, досліджуючи адміністративно-правове регулювання інформаційних відносин в Україні, зазначає, що правові відносини, що виникають у публічній сфері суспільства та держави в ході одержання, використання, поширення та зберігання інформації, характеризуються значним динамізмом і нестабільністю правової регламентації. Забезпечуючи різноманітні суспільні процеси, окремі групи цих відносин в результаті трансформації моделі відносин між органами державної влади та громадянами з часом втрачають свою актуальність та зазнають кардинальних змін (відносини у сфері надання адміністративних послуг, електронного урядування, електронної демократії та ін.). Таким чином, постійно змінюючись і коригуючись, система публічних потреб в інформаційній сфері сприяла змінам і коригуванню адміністративно-правових норм. Це, у свою чергу, зумовлює виникнення нових або оновлення суспільних відносин у владно-управлінській сфері (перш за все у сфері обігу інформації) [31, с. 3].

Таким чином, адміністративно-правове регулювання інформаційних відносин вирізняється особливим динамізмом, адже інформаційні технології постійно змінюються, удосконалюються, з'являються кардинально нові цифрові інструменти, що в сукупності вимагає від суб'єктів нормотворчої діяльності постійного моніторингу новел цифрового життя, а також дослідження впливу нових інформаційних технологій на існуючі суспільні відносини, пошуку можливості їх використання для удосконалення технологічних процесів та механізму публічного управління.

На думку С. Єсімова, на сучасному етапі розвитку суспільства потоки інформації зростають з кожним днем, причому як загалом у країні, так і всередині окремих галузей управління. Такі процеси ведуть до глобалізації світового простору, трансформуючи його. У зв'язку з цим особливої актуальності набувають дії суб'єктів права не тільки в звичайному фізичному просторі, а й в інформаційному. Інформаційний простір формується не тільки завдяки розвитку інформаційних технологій, але й на основі відповідних нормативних актів [107, с. 25].

Крім того, С. Єсімов слушно зазначає, що у системі державних органів і в управлінських процесах інформаційні технології виступають сполучними ланками, що забезпечує взаємодію і інтеграцію всіх рівнів і елементів системи та виконання нею (і її інститутами) всіх основних функцій. Механізми використання інформаційних технологій мають адміністративно-організаційні, адміністративно-правові й інформаційно-комунікаційні складові. Особливість адміністративно-правової складової механізму використання інформаційних технологій у сфері державного управління полягає в тому, що він поки що на етапі свого формування. Впровадження сучасних інформаційних технологій забезпечує цілісність інформаційної сфери, що розвивається згідно з певними закономірностями. Якщо ігнорувати закономірності розвитку інформаційної сфери, то знижується дієвість рішень, зменшується ефективність впровадження інформаційних систем в роботу органів влади, виникає необхідність реформування системи управління.

Інформаційне забезпечення якісно і ефективно реалізується тільки в умовах наявності достатнього адміністративно-правового регулювання використання інформаційних технологій. Розроблення та впровадження адміністративно-правового регулювання використання інформаційних технологій сприяють переходу до нової суспільної формації – інформаційного суспільства. Отже, адміністративно-правове регулювання використання інформаційних технологій забезпечує ефективне державне управління на всіх рівнях [107].

Таким чином, адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності забезпечить ефективне державне управління на всіх рівнях механізму забезпечення життєдіяльності та єдиної державної системи цивільного захисту.

О. Кузьменко, В. Чорна та С. Островський за результатами дослідження правового регулювання запровадження та використання штучного інтелекту, як провідної інформаційної технології, зазначають, що впровадження правового регулювання штучного інтелекту є критично важливим для забезпечення його безпечного та етичного використання. Міжнародна співпраця та гармонізація нормативних рамок можуть сприяти створенню ефективної системи регулювання, що враховує інтереси всіх сторін і сприяє розвитку інновацій, одночасно захищаючи права та свободи людини [157, с. 176-177].

Отже, правове регулювання використання інформаційних технологій, включаючи технологію штучного інтелекту, є умовою їх безпечного використання, тобто використання з дотриманням основних правил безпеки життєдіяльності, включаючи запобігання можливому негативному впливу на людину та навколишнє природне середовище.

О. Олійник слушно зазначає, що захист інформаційних ресурсів є одним із пріоритетних завдань органів публічної адміністрації, які реалізують державну політику у сфері національної безпеки України. В умовах постіндустріального етапу розвитку суспільства інформація, інформаційні

ресурси перетворились на: стратегічний ресурс економічного і науково-технологічного прогресу, життєдіяльності і розвитку соціальних і біологічних систем; важливий фактор успішної внутрішньої і зовнішньої політики та національної безпеки; об'єкт виробництва, товарних відносин і конкуренції [190, с. 1].

Варто погодитись із вищенаведеною позицією О. Олійника, адже захист інформаційних ресурсів є неодмінною (органічною) складовою загального механізму забезпечення безпеки життєдіяльності. Інформація в цифровому (цифровізованому) світі є не тільки товаром, а інформаційні технології не тільки засобом виробництва. Інформація про особу стає частиною світової мережі та може бути використана з негативною метою, спотворена або знищена, що в умовах цифровізації суспільних відносин може завдати суттєвої шкоди людині, значно порушити умови її нормальної життєдіяльності. Масштабні інформаційні атаки порушують умови нормальної життєдіяльності всього суспільства та становлять загрозу національній безпеці. Саме тому правова регламентація структури та порядку функціонування механізму захисту інформаційних ресурсів є пріоритетним завданням суб'єктів законотворчої та нормотворчої діяльності.

На думку А. Омельченка, законодавство про цифровізацію слід розглядати у широкому та вузькому значенні. У широкому значенні до системи законодавства про цифровізацію слід віднести інформаційне законодавство, законодавство про електронні комунікації та радіочастотний ресурс, про інформатизацію, про надання електронних довірчих послуг, про електронну комерцію, про захист персональних даних, про кібербезпеку. У вузькому значенні до такого законодавства слід відносити нормативно-правові акти, предметом регулювання яких є безпосередньо відносини у сфері цифровізації [191, с. 40].

Таким чином, науковці приділяють значну увагу правовому регулюванню інформаційних відносин (включаючи питання використання нових інформаційних технологій), розвитку інформаційного законодавства в

цілому, що свідчить про позитивну тенденцію активізації наукових досліджень, які покликані створити надійну теоретико-методологічну основу розвитку правових засад цифровізації.

Четверта група – дослідження науковців, присвячені організації публічного управління та правовому регулюванню у сфері забезпечення безпеки життєдіяльності.

Із останніх досліджень у даній сфері слід відзначити публікації Ф. Апшая та О. Халака «Аналіз правових засад безпеки життєдіяльності» [11], В. Глухої та А. Помази-Пономаренко «Нормативно-правове забезпечення державного управління сферою безпеки життєдіяльності» [75], А. Денисової «Напрями адміністративного нагляду у сфері забезпечення безпеки життєдіяльності населення: питання систематизації» [92], О. Остапенка «Адміністративно-правова природа безпеки населення України» [197].

Так, Ф. Апшай та О. Халак зазначають, що найважливішою складовою вирішення проблеми забезпечення економічної, соціальної та військової безпеки держави є навчання населення громадянської обороні та захисту від надзвичайних ситуацій. Суттєве значення у зазначеному контексті також мають питання прищеплення населенню належного рівня розуміння культури безпеки життєдіяльності. У сучасних умовах необхідно виходити з необхідності консолідації всіх національних сил: державних, приватних та громадських. Формування культури безпеки життєдіяльності у країні та правових засад цього процесу потребує його належного регулювання на державному рівні. Головними чинниками цього процесу повинні стати розробка з боку держави певних нормативних актів, що регулюють усі питання у цьому напрямку та створюють належні умови щодо правового захисту праці у країні [11, с. 6].

Таким чином, вчені наголошують на необхідності правового регулювання формування культури безпеки життєдіяльності, включаючи навчання населення громадянської обороні та захисту від надзвичайних ситуацій. Правове регулювання вказаних правовідносин покликане

забезпечити уніфіковані підходи до вирішення питань забезпечення безпеки життєдіяльності та гарантувати поширення відповідного локального позитивного досвіду на територію всієї держави.

В. Глуха та А. Помаза-Пономаренко акцентують увагу на тому, що значна увага до проблем забезпечення безпеки життєдіяльності приділяється сьогодні як науковцями, так і керівництвом держави. Це обумовлене концентрацією різноманітних ресурсів у межах окремо взятої території, які виступають головним потенціалом країни в контексті інтеграційних прагнень нашої держави. Разом із тим, вирішення останнього завдання видається можливим за умови кардинального оновлення механізмів державного управління, зокрема регіонального, які залишаються економічно неефективними, а також подекуди соціально, технологічно й екологічно небезпечними, що призводить до виникнення небезпеки найважливішим сферам життєдіяльності [75].

Варто погодитись із такою позицією науковців, адже механізми державного управління, зокрема регіонального, дійсно потребують кардинального оновлення з урахуванням останніх досягнень у сфері інформаційних технологій. Наприклад, все більшої актуальності набуває питання використання технології штучного інтелекту для удосконалення механізму публічного управління суспільними відносинами, включаючи сферу забезпечення безпеки життєдіяльності в цілому та систему цивільного захисту зокрема. На окрему увагу заслуговує питання здійснення адміністративного нагляду у зазначених сферах суспільних відносин.

А. Денисова слушно зауважує, що адміністративний нагляд у сфері забезпечення безпеки життєдіяльності населення здійснюється за багатьма напрямами (видами), перелік яких у жодному нормативно-правовому акті не встановлений. Разом із тим існує нагальна потреба визначення тих видів життєдіяльності населення, забезпечення безпеки яких об’єктивно потребує здійснення адміністративного нагляду [92, с. 156].

Крім того, А. Денисова зазначає, що адміністративний нагляд у сфері забезпечення життєдіяльності населення умовно можна поділити на два ключових напрями: загальний адміністративний нагляд, здійснення якого пов'язане зі створенням умов провадження підприємництва, гарантування безпечного середовища проживання населення; спеціальний адміністративний нагляд, який здійснюється у певних сферах життєдіяльності (охоронна діяльність; правила використання предметів і речовин з обмеженим доступом; окремі сфери підприємництва тощо). За такою систематизацією до загального адміністративного нагляду у сфері забезпечення життєдіяльності населення доцільно віднести, зокрема, державний санітарно-епідеміологічний нагляд, державний нагляд (контроль) у сфері екології, нагляд у сферах пожежної і техногенної безпеки, нагляд (контроль) в інформаційній сфері [92, с. 159].

Таким чином, актуальним є питання чіткого адміністративно-правового регулювання здійснення адміністративного нагляду у сфері забезпечення безпеки життєдіяльності населення, включаючи детальну класифікацію його основних напрямів (видів). Детальна адміністративно-правова регламентація адміністративного нагляду у сфері забезпечення безпеки життєдіяльності покликана усунути корупційні фактори та створити чіткі і прозорі умови та правила взаємодії суб'єктів господарської діяльності із органами публічної адміністрації, які реалізують державну політику у сфері цивільного захисту.

О. Остапенко слушно зауважує, що сучасний стан захищеності населення від загроз і ризиків потребує, насамперед, уваги від держави щодо своєчасного та ефективного застосування правових засобів захисту. Чинне законодавство України, у тому числі й адміністративне, містить певний перелік норм, що передбачають захист від посягань на права, здоров'я і свободу громадян, на національні та державні інтереси у сфері безпеки. Адміністративно-правова природа безпеки населення України, як правило, розглядається як захист від протиправних посягань на фізичну особу, матеріальні цінності. Разом з тим, наголошує О. Остапенко, існують інші види загроз природного і техногенного змісту, що є небезпечними для суспільства

й держави, і потребують вивчення їх природи та адміністративно-правового регулювання відносин у сфері безпеки [197, с. 235].

Крім того, на думку О. Остапенка, юридичну природу і зміст безпеки варто розглядати як один із засобів, за допомогою якого є можливість протидії шкідливим та небезпечним екологічним, біологічним, техногенним та іншим загрозам, що впливають на навколишнє природне середовище, у якому перебуває фізична особа. Одним з правових інструментів забезпечення і регулювання відносин у сфері безпеки є адміністративне право [197, с. 235].

Із такою позицією варто погодитись, адже адміністративне право володіє потужним правовим інструментарієм регулювання суспільних відносин, включаючи як засоби заохочення, так і заходи адміністративного примусу, які поділяються на три основні види: заходи адміністративного припинення, адміністративно-запобіжні заходи та заходи адміністративної відповідальності.

Наведені вище літературні джерела відображають лише частину наукових досліджень у сферах інформаційного права, безпеки життєдіяльності та цивільного захисту, адміністративно-правового регулювання забезпечення безпеки життєдіяльності, адже питання безпеки суспільства, захисту людини від негативних чинників природного, техногенного, соціального та воєнного характеру, а також питання використання інформаційних технологій з метою удосконалення існуючих суспільних відносин присутні у значній кількості сучасних наукових робіт, виконаних в рамках спеціальностей як природничих та технічних наук, так і в рамках галузі адміністративного права.

В межах окремого дисертаційного дослідження неможливо охопити та проаналізувати увесь масив наукових досліджень, присвячених означеним питанням, проте вищезазначені роботи вже дають підстави для висновку про формування чіткої тенденції щодо активізації наукових досліджень питань адміністративно-правового регулювання використання інформаційних технологій та забезпечення безпеки життєдіяльності.

Таким чином, для дослідження питання адміністративно-правового

забезпечення використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності необхідно використовувати широке коло нормативних та літературних джерел, наукових робіт фахівців з технічних, природничих наук та юриспруденції.

На окрему увагу заслуговує визначення методології дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, адже від правильно підібраного методологічного інструментарію залежить ефективність наукового пошуку та його результативність.

1.2 Методологія дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності

Проведення змістовного наукового дослідження потребує визначення інструментарію наукового пошуку, який буде застосовуватись в процесі підготовки наукової роботи. Питанням методології наукового пошуку присвятили свою увагу представники різних спеціальностей, включаючи вчених-юристів. Так, методології правових наукових досліджень присвятили свою працю О. Ганьба та В. Мірошниченко [73], методологічні основи дослідження права у сучасній юридичній науці охарактеризувала Г. Лук'янова [170], методологічні проблеми сучасних правових досліджень проаналізувала Н. Кушакова-Костицька [162], становлення та основні напрями розвитку методології сучасного правознавства дослідив М. Кельман [132].

В контексті теми дослідження на увагу заслуговує публікація В. Пашинського «Методологічний інструментарій дослідження проблем адміністративно-правового забезпечення оборони держави» [202].

В самій назві останньої публікації простежується інструментальний підхід, тобто методологія дослідження розглядається як набір реальних засобів-інструментів наукового пошуку, які використовуються з конкретною

метою – детально та всебічно дослідити, наприклад, певне правове явище чи процес та сформулювати конкретні практичні пропозиції щодо удосконалення чинного національного законодавства та юридичної практики.

Основну увагу методології досліджень правових явищ та процесів приділяють теоретики держави та права. Так, П. Рабінович під методологію юридичної науки пропонує розуміти систему підходів і способів наукового дослідження, теоретичні засади їх використання при вивченні державно-правових явищ [293, с. 618].

Наведене визначення є лаконічним та відображає саму суть методології юридичної науки. Метою дослідження не повинно бути само дослідження, коли автор попадає в безкінечний процес протиставлення чужих думок та в результаті не досягає будь-якого науково та практично значимого результату. Саме тому важливим є правильний вибір підходів та способів наукового дослідження, а також чітке формулювання теоретичних засад їх використання в процесі наукового пошуку.

Д. Голосніченко слушно зауважує, що методологія дослідження в юридичній науці є не простим набором певних основоположних понять та категорій, прийомів і методів дослідження. Методологія, на його думку, є теоретичним обґрунтуванням доцільності застосування відповідних підходів і способів, які використовуються для проведення певного теоретико-юридичного дослідження, а також дібрана на науковій основі для означеної мети система прийомів і способів, тобто відповідних методів» [77, с. 10].

Таким чином, Д. Голосніченко наголошує на необхідності теоретичного обґрунтування доцільності застосування певних підходів і способів наукового пошуку. В процесі розвитку юридичної науки накопичено значну кількість наукових підходів, прийомів та способів, тобто методів наукових досліджень, тому науковцю важливо не розгубитися в масивах наукових рекомендацій та постулатів, сформованих різними науковими юридичними школами. Саме тому теоретичне обґрунтування доцільності застосування певних підходів і способів дослідження конкретного державно-правового явище чи процесу

повинно бути першою сходинкою на шляху наукового пошуку.

В свою чергу Д. Тихомиров приділяє увагу конкретним науковим підходам і зазначає, що основними методологічними положеннями застосування діяльнісного підходу є те, що діяльність носить цілеспрямований характер та здійснюється в певних конкретно-історичних та соціально-культурних умовах (кожен етап існування суспільства характеризується певними особливостями, що зумовлено кліматичними умовами, нездоланними природними та техногенними явищами, рівнем науково-технічного прогресу тощо). Також діяльність спрямована на забезпечення суспільних та власних потреб суб'єкта, при цьому вона впорядковується різноманітними соціальними регуляторами, а також внутрішніми переконаннями її суб'єкта. У процесі здійснення діяльності використовуються різноманітні засоби [311, с. 231].

Таким чином, діяльнісний підхід не виключає, а, навпаки, передбачає необхідність та доцільність використання інших методів – системного, структурного, функціонального, статистичного, а також психологічних, конкретно-соціологічних та інших, і може бути застосований до різних правових динамічних явищ [311, с. 231; 86, с. 4-5].

Таким чином, забезпечення безпеки життєдіяльності та цивільний захист необхідно розглядати як діяльність уповноважених суб'єктів владних повноважень та інших суб'єктів, спрямовану на створення безпечного середовища для людини та суспільства в цілому. Відповідно, напрями та способи удосконалення такої діяльності з використанням цифрових (інформаційних) технологій становлять предмет даного дослідження.

Системний підхід, на думку Д. Тихомирова, розуміється як сукупність предметів і явищ навколишнього світу, за якої вони розглядаються як частини або елементи певного цілісного утворення. За системного підходу частини або елементи системи розглядається як окремо, так і у взаємодії між собою, внаслідок чого визначаються особливості системного явища, що можуть бути відсутні в окремих його елементах [311, с. 232].

В контексті теми даного дослідження системний підхід дозволяє розкрити та охарактеризувати всі елементи механізму забезпечення безпеки життєдіяльності та єдиної державної системи цивільного захисту. Крім того, системний підхід дозволяє систематизувати положення чинного національного законодавства, якими врегульовано різні аспекти використання інформаційних технологій у сфері забезпечення безпеки життєдільності та цивільного захисту.

В свою чергу функціональний підхід надає можливість враховувати напрями впливу на суспільні відносини під час реалізації державної політики [311, с. 234]. Так, функціональний підхід дозволяє охарактеризувати функції всіх органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, та інших суб'єктів, які задіяні в механізмі забезпечення безпеки життєдіяльності.

Порівняльно-правовий підхід бере за основу порівняння вже досліджених правових явищ для виявлення розбіжностей та схожих рис вказаних явищ [311, с. 234]. Так, порівняльно-правовий підхід дозволяє показати особливості правового регулювання у сфері забезпечення безпеки життєдіяльності та у сфері цивільного захисту, різницю між ними та взаємозв'язок.

Методологія дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності ґрунтується на органічному поєднанні філософських, загальнонаукових та спеціально-юридичних методів дослідження.

Так, серед філософських методів більшою мірою використовується метод діалектики, його закони та прийоми. Так, закон єдності та боротьби протилежностей найбільш ярко проявляється у суспільних відносинах, пов'язаних із безпекою життєдіяльності, адже штучне соціальне середовище, створене людиною, вступає у певне протиріччя із навколишнім природним середовищем, природніми процесами та явищами. Наприклад, природні лісові пожежі, виверження вулканів, землетруси сприймаються людиною як

катастрофічні надзвичайні ситуації, які руйнують створене людиною середовище та порушують нормальні умови людського життя.

Проте, саме завдяки заходам забезпечення безпеки життєдіяльності та їх правовому забезпеченню досягається компроміс між двома протилежностями – природними та соціальними процесами, створюються умови, за яких людина може завчасно виявити та попередити інших про небезпеку виникнення надзвичайної ситуації, а також мінімізувати її негативні наслідки.

І саме завдяки інформаційним технологіям суспільство отримало можливість автоматизувати процеси завчасного попередження про загрозу настання небезпечної ситуації, а також можливість оперативно мобілізувати людські та матеріально-технічні ресурси для ліквідації самої надзвичайної ситуації та її наслідків.

Таким чином, правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності необхідно здійснювати із урахуванням вказаного закону діалектики – єдності та боротьби протилежностей.

Також в процесі дослідження вказаної тематики доцільно використовувати закон переходу кількісних змін у якісні. Так, системне внесення змін до чинного законодавства, розробка проектів нових нормативно-правових актів в результаті повинні привести до якісних змін в правовому регулюванні використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Причому ключову роль відіграє не формальна кількість внесених змін, а саме узгоджена та наполеглива нормотворча діяльність уповноважених суб’єктів органів публічної адміністрації. Так, в процесі правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності суб’єктам нормотворчості органів державної влади, які реалізують державну політику у сфері цивільного захисту, доцільно узгоджувати свої розробки із представниками Міністерства цифрової трансформації України, що забезпечить правову регламентацію застосування останніх досягнень у сфері

цифрових технологій для забезпечення безпеки життєдіяльності, захисту населення та територій від надзвичайних ситуацій.

Також в процесі дослідження даної тематики доцільно застосувати прийом «заперечення заперечення». Вказаний прийом дозволяє досліднику йти від зворотного, тобто з початку заперечувати необхідність правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а потім аргументовано спростовувати власне заперечення – доводити необхідність внесення відповідних змін до чинного законодавства або прийняття нових законів чи підзаконних нормативно-правових актів. Так, з одного боку, цифрові інструменти у більшості своїй є загальнодоступними та можуть використовуватися усіма суб'єктами правовідносин, проте, якщо розглядати діяльність у сфері забезпечення безпеки життєдіяльності, яка здійснюється більшою мірою уповноваженими особами органів публічної адміністрації, то необхідно згадати положення ст. 19 Конституції України, згідно з якими органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України [149].

Таким чином, використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності потребує належної адміністративно-правової регламентації, що не тільки забезпечить дотримання Конституції України, але й дозволить поширювати локальний позитивний досвід використання інформаційних технологій у вказаній сфері суспільних відносин на територію всієї держави.

Окрім вищезазначених законів та прийомів методу діалектики в процесі дослідження необхідно застосовувати такі його принципи як принцип об'єктивності та принцип історизму.

Принципи об'єктивності передбачає використання верифікованих даних, зокрема, офіційно оприлюднених текстів нормативно-правових актів та іншої інформації органів публічної адміністрації, даних репрезентативних

соціологічних досліджень, які охоплюють широкі верстви населення із правильно проведеною вибіркою респондентів тощо. Дотримання принципу об'єктивності також передбачає дослідження можливості використання у сфері забезпечення безпеки життєдіяльності тих інформаційних технологій, які вже пройшли перевірку на практиці та відповідними фахівцями підтверджено доцільність їх використання. Враховуючи особливе значення систем забезпечення життєдіяльності та цивільного захисту для збереження життя та здоров'я людей, використання неперевірених цифрових продуктів, зокрема, програмного забезпечення, може призвести до катастрофічних наслідків. Наприклад, через помилки в програмному забезпеченні не спрацює автоматизована система захисту на атомній електростанції або протипожежна сигналізація з автоматичною системою пожежогасіння тощо.

Принцип історизму передбачає врахування в процесі дослідження тих історичних умов, за яких було здійснено правове врегулювання тих або інших суспільних відносин, зокрема, політичних, економічних та соціальних факторів, які вплинули або могли вплинути на суб'єкта нормотворчої діяльності. Так, питання адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності виникає лише на тому історичному етапі, коли рівень розвитку інформаційних технологій дозволив використовувати їх з практичною метою, зокрема, у сфері забезпечення безпеки життєдіяльності. Збільшення кількості цифрових інструментів автоматизації систем цивільного захисту обумовило необхідність їх стандартизації, ліцензування, правової регламентації їх впровадження в діяльність органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту.

Серед загальнонаукових методів для дослідження актуальних питань адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності більшою мірою необхідно використовувати прийми логіки, а саме – аналіз, синтез, дедукцію та індукцію, а також системний та структурно-функціональний методи,

прийоми соціологічного методу та метод статистики.

Так, за допомогою прийомів логіки аналізується сучасний стан адміністративно-правового забезпечення використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, за допомогою дедукції та індукції визначаються ті суспільні відносини, які потребують правого врегулювання, а за допомогою синтезу використовуються спеціальні знання у сфері інформатизації, використання інформаційних технологій для удосконалення механізму забезпечення безпеки життєдіяльності, попередження та ліквідації надзвичайних ситуацій тощо.

Системний метод дозволяє провести систематизацію міжнародних та національних нормативно-правових актів, які так чи інакше регулюють суспільні відносини, пов'язані із використанням інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Крім того, системний метод дозволяє систематизувати всі наявні засоби забезпечення безпеки життєдіяльності та цивільного захисту, а також цифрові інструменти, які можуть бути використані для оптимізації механізму забезпечення безпеки життєдільності, та виокремити ті із них, які потребують адміністративно-правової регламентації.

В свою чергу структурно-функціональний метод дозволяє визначити структуру механізму забезпечення безпеки життєдіяльності та функції кожного з елементів з урахуванням наявності або відсутності відповідних адміністративно-правових засад функціонування вказаних елементів. Наприклад, єдина державна система цивільного захисту є достатньо складною багаторівневою структурою органів публічної адміністрації, а також підприємств, установ та організацій, які забезпечують реалізацію державної політики у сфері цивільного захисту. Кожен суб'єкт єдиної державної системи цивільного захисту має свої, чітко визначені законодавством, функції, реалізація яких дозволяє досягти мети правового регулювання функціонування вказаної системи та забезпечити належний рівень цивільного захисту населення і територій від надзвичайних ситуацій та їх наслідків.

На окрему увагу заслуговує використання соціологічного методу для дослідження питання адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Такі прийоми соціологічного методу як опитування та анкетування дозволяють визначити рівень довіри суспільства до органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, ставлення громадян до тих або інших напрямків та способів діяльності держави щодо запобігання виникненню надзвичайних ситуацій, а також щодо мінімізації та ліквідації їх наслідків. І саме сучасні інформаційні технології дозволяють оперативно проводити соціологічні дослідження з охопленням максимальної кількості респондентів шляхом, зокрема, проведення опитувань в соціальних мережах, на сайтах засобів масової інформації та органів публічної адміністрації (наприклад, на Єдиному порталі державних послуг Дія), а також із використанням мобільних застосунків. За допомогою таких опитувань можна встановити ставлення громадян до можливих варіантів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, наприклад, щодо бажання та готовності встановити автоматизовану протипожежну сигналізацію та автоматичну систему пожежогасіння за місцем проживання або роботи, щодо доцільності облаштування або планування при будівництві нових об’єктів нерухомості автоматизованих індивідуальних кімнат-укриттів (бомбосховищ) з системами життєзабезпечення тощо.

Метод статистики дозволяє використовувати офіційну статистичну інформацію щодо кількості надзвичайних ситуацій та їх видів, які мали місце протягом певного періоду, кількості проведених (реалізованих) заходів цивільного захисту, спрямованих на запобігання виникненню та ліквідацію наслідків надзвичайних ситуацій, кількості особового складу органів публічної адміністрації та добровольців, задіяних в реалізації вказаних заходів тощо. Також за допомогою методу статистики можна виявити тенденції щодо впровадження інформаційних технологій в діяльність органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту,

зокрема, за допомогою Звітів про основні результати діяльності Державної служби України з надзвичайних ситуацій за попередні роки, які розміщені на офіційному веб-сайті вказаної державної служби.

Серед спеціально-юридичних методів дослідження особливу увагу необхідно приділити методу порівняльного правознавства, формально-юридичному методу та методу юридичного моделювання.

Так, метод порівняльного правознавства дозволяє порівняти національне законодавство та законодавство зарубіжних країн в частині адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, виокремити відповідний позитивний досвід зарубіжних країн та визначити можливість та доцільність його запозичення з метою імплементації в національне законодавство та юридичну практику.

Формально-юридичний метод або метод юридичної догматики є по суті похідним від загальнонаукового аксіоматичного методу дослідження. Він дозволяє використовувати певні юридичні аксіоми, на основі та з використанням яких вибудовується увесь механізм правового регулювання. До таких аксіом відносяться зокрема принципи верховенства норм ратифікованих міжнародно-правових актів над відповідними нормами національного законодавства, верховенство фундаментальних прав і свобод людини над інтересами держави, неприпустимість втручання у сферу особистої (інтимної) свободи людини тощо. Так аксіомою є закріплене в Конституції України положення про те, що забезпечення екологічної безпеки і підтримання екологічної рівноваги на території України, подолання наслідків Чорнобильської катастрофи – катастрофи планетарного масштабу, збереження генофонду Українського народу є обов’язком держави (ст. 16 Конституції України) [149].

Також аксіомою (юридичною догмою) є положення ст. 3 Конституції України про те, що людина, її життя і здоров’я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною

цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави [149].

Таким чином, однією із найвищих соціальних цінностей в Україні є безпека людини і забезпечення безпеки кожної людини та суспільства в цілому в сукупності з іншими правами і свободами людини визначають зміст і спрямованість діяльності держави, основні напрями її політики.

Так, у відповідності до ст. 50 Конституції України, кожен має право на безпечне для життя і здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди. Кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена [149].

Наведені правові аксіоми є основою побудови та функціонування національного механізму забезпечення безпеки життєдіяльності та єдиної державної системи цивільного захисту.

В свою чергу метод юридичного моделювання дозволяє змоделювати та сформулювати конкретні пропозиції щодо актуальних напрямів та способів удосконалення чинного національного законодавства, а також розробки перспективних нормативно-правових актів щодо адміністративно-правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Адже метою будь-якого наукового дослідження має бути не тільки формулювання загальнотеоретичних положень, але й напрацювання конкретних пропозицій щодо внесення змін до чинних законів або щодо прийняття положень перспективного законодавства.

Окрему увагу необхідно приділити науковим підходам, які доцільно використовувати в процесі дослідження обраної тематики.

Так, цивілізаційний підхід передбачає урахування під час дослідження зарубіжного досвіду адміністративно-правового регулювання використання

інформаційних технологій у сфері забезпечення безпеки життєдіяльності національних правових традицій та звичаїв, особливостей національної правосвідомості та правової культури, яка сформована під впливом певних цивілізаційних чинників, а також урахування правових традицій та звичаїв, особливостей суспільної правосвідомості та правової культури тієї держави, досвід якої у певній сфері правового регулювання досліджується. Так, слід відзначити, що Україна безумовно відноситься до Західної цивілізації, тому пріоритетним напрямом нормотворчої діяльності органів публічної адміністрації має бути адаптація національного законодавства до норм та принципів права Європейського Союзу як найбільшого державно-правого та безпекового утворення західної цивілізації. Крім того, в національному механізмі забезпечення безпеки життєдіяльності та єдиній державній системі цивільного захисту обов'язково необхідно враховувати загрози безпеці громадян України, які походять з боку Східної цивілізації, зокрема союзу російської федерації з іншими недемократичними утвореннями Сходу. Особливу увагу необхідно приділяти ролі інформаційних технологій як ключовому фактору розвитку сучасної цивілізації та інструменту протидії загрозам з боку сусідніх держав.

Телеологічний науковий підхід вимагає від дослідника не здійснювати дослідження заради самого дослідження. Науковий пошук повинен мати конкретну мету, до прикладу – розробку конкретних пропозицій щодо внесення змін до чинного національного законодавства або пропозиції щодо розробки перспективного нормативно-правового акту. Так, щодо правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності важливо забезпечити як теоретичну, так і практичну значимість проведеного дослідження. Крім того, телеологічний науковий підхід передбачає визначення чіткої мети використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а саме – удосконалити національний механізм забезпечення безпеки життєдіяльності та систему цивільного захисту шляхом максимальної автоматизації

відповідних процесів та мінімізації ролі людини в управлінні вказаними процесами.

Інструментальний підхід дозволяє розглядати механізм забезпечення життєдіяльності як систему дієвих засобів запобігання негативним факторам, які впливають або можуть вплинути на життєдіяльність людини та нормальне функціонування суспільства в цілому, а також засобів ліквідації надзвичайних ситуацій та їх наслідків.

В свою чергу право з точки зору інструментального підходу є не тільки системою заборон, зобов'язань та дозволів, а й системою правових засобів (інструментів) досягнення публічної чи приватної мети учасників суспільних відносин. Таким чином, адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності розглядається як дієвий правовий інструмент оптимізації та удосконалення механізмів забезпечення безпеки життєдіяльності та цивільного захисту.

Синергетичний науковий підхід передбачає дослідження механізму правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності як складної системи, що прагне до самоорганізації та самовдосконалення, адже кожен уповноважений суб'єкт владних повноважень, який здійснює нормотворчу діяльність у вказаній сфері суспільних відносин, повинен узгоджувати свої дії, проєкти з іншими суб'єктами і результатом такої спільної діяльності (об'єднання зусиль) повинен бути синергетичний ефект – розробка та прийняття якісного та ефективного законодавства, практична реалізація якого задовольнить як публічні, так і приватні інтереси учасників правовідносин.

На думку Ю. Орлова, О. Джужи та О. Орлової одним із прогресивних і продуктивних методів сучасної науки є синергетика. Термін «синергетика» (від грецького «synergetikos» – спільний; той, що діє узгоджено) було запропоновано німецьким ученим Германом Хакеном, який розумів під ним науковий метод, що дає змогу пояснити механізм «спонтанного» виникнення структур у складній системі внаслідок взаємодії між її елементами [98].

Причому спонтанне виникнення структур у складній системі не означає, що вказані структури виникають хаотично, безпричинно. Синергетика передбачає багатофакторний вплив на кожен з елементів складної системи і саме такий вплив призводить до самоорганізації системи, коли начебто розрізнені елементи вибудовуються в чітку ієрархічну структуру. Так, механізм забезпечення безпеки життєдіяльності включає в себе велику кількість сил та засобів, інструментів забезпечення безпеки кожної людини та суспільства в цілому, причому вказані інструменти, їх особливості обумовлені характеристиками тих негативних факторів, які зумовлюють виникнення надзвичайної ситуації – пожежі, повені, землетрусу, техногенної катастрови, соціального чи збройного конфлікту тощо.

Синергетика вивчає зв'язки між елементами структури (підсистемами), утвореними у відкритих системах (фізико-хімічних, біологічних, соціальних, психологічних, технічних) завдяки інтенсивному (потоковому) обміну речовиною й енергією з навколишнім середовищем у нерівномірних умовах. У таких системах спостерігається узгоджена поведінка підсистем, у результаті чого зростає ступінь їх упорядкованості, тобто зменшується ентропія. Цей процес має природничо-наукову сутність і позначається терміном «самоорганізація». Теоретичну основу синергетики становлять термодинаміка нерівноважних процесів, теорія випадкових процесів, теорія нелінійних коливань і хвиль. Істотна відмінність синергетики від інших традиційних методів наукового пізнання полягає в тому, що вона, вивчаючи складні системні утворення, досліджує не сутність складових частин (елементів) цих систем (що є змістом класичного наукового аналізу), а, насамперед, характер системних зв'язків між цими елементами. Такий підхід дає незвичайні результати, головним із яких, вочевидь, є відкриття універсальних закономірностей, однаково властивих усім системним утворенням незалежно від рівня складності їх елементів: фізичних, хімічних, біологічних, екологічних, психологічних, соціальних, технічних. Така універсальність, ізоморфність законів синергетики поступово сприяє формуванню мови

загальнонаукового, міждисциплінарного рівня, що дає змогу краще розуміти один одного представникам точних і гуманітарних наук: фізику й соціологу, техніку та юристу [193, с. 76].

Отже, особливе значення синергетика, синергетичний науковий підхід має в процесі дослідження механізму забезпечення безпеки життєдіяльності, адже безпека життєдіяльності є міждисциплінарною науковою та навчальною дисципліною, яка об'єднує, систематизує та взаємопов'язує знання з фізики, хімії, біології, соціології, військової справи. В свою чергу юриспруденція охоплює всі питання, пов'язані із правовим регулюванням застосування спеціальних технічних міждисциплінарних знань для забезпечення безпеки життєдіяльності людини та суспільства в цілому, включаючи використання інформаційних технологій у вказаній сфері суспільних відносин. Таким чином, саме юридична наука забезпечує той синергетичний ефект, який полягає у встановленні та характеристиці системних зв'язків між окремими елементами механізму забезпечення безпеки життєдіяльності та системи цивільного захисту, наданні їм правової форми та забезпеченні реалізації з боку держави (засобами заохочення та примусу).

Науковці зазначають, що синергетичні закономірності спостерігаються також у процесах адаптації чинних нормативних актів до мінливих суспільних потреб шляхом унесення до них змін і доповнень. У цьому разі зміст нормативного акта має бути приведено до стану максимальної відповідності сучасним соціальним потребам, тобто, говорячи мовою синергетики, до стану-атрактору. Особливістю такого процесу є те, що він здійснюється «покроково» (дискретно). На відміну від нього, процес формування суспільних потреб можна умовно вважати безперервним. Тому між соціальними відносинами, що потребують правового регулювання, і відповідними правовими нормами завжди існує «дистанція», яка показує «відставання» права від соціальних реалій, а також, зростаючи з часом на локальному рівні, породжує в суспільстві хаотичні явища та нестійкі (біфуркаційні) стани. Ця «дистанція» є головною причиною правотворчості як діяльності щодо впорядкування

суспільних відносин. «Відставання» правових норм від соціальних потреб спричиняє появу елементів самоорганізації у сфері застосування права [193, с. 82].

Особливо «відставання» правових норм від соціальних потреб проявляється у сфері правового регулювання використання інформаційних технологій, адже майже щодня з'являються нові інформаційні технології, які оперативно впроваджуються в практичну діяльність (відбувається самоорганізація в механізмі правового регулювання), проте часто-густо вказані технології потребують належної правової регламентації в силу специфіки їх застосування на практиці, а також потенційного впливу на права і свободи людини.

Таким чином, змістовне та всебічне дослідження актуальних питань адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності необхідно здійснювати із використанням інструментарію філософських, загальнонаукових та спеціально-юридичних методів дослідження, а також провідних наукових підходів, серед яких більшою мірою доцільно застосовувати цивілізаційний, телеологічний та синергетичний підходи.

Також слід відзначити, існуючий стан адміністративно-правового регулювання систем забезпечення безпеки життєдіяльності та цивільного захисту в Україні потребує удосконалення, адже єдина державна система цивільного захисту функціонує в умовах правового режиму воєнного стану та зтикається з новими викликами та загрозами, зумовленими розвитком інформаційного суспільства, появою нових інформаційних технологій, використання яких потребує правової регламентації.

Водночас для формулювання конкретних пропозицій щодо удосконалення чинного адміністративного законодавства у сфері правового регулювання систем забезпечення безпеки життєдіяльності та цивільного захисту, а також використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, важливо чітко розмежувати вказані

поняття, визначити особливості адміністративно-правового регулювання відповідних суспільних відносин.

Безпека життєдіяльності є широким поняттям, яке охоплює всі аспекти захисту життя та здоров'я людини, суспільства в цілому, а також навколишнього природного середовища від природних, техногенних та інших небезпек. Саме тому безпека життєдіяльності викладається як окрема навчальна дисципліна у навчальних закладах, а також є окремою наукою про способи «виживання» людини у світі, наповненому негативними чинниками, загрозами різного характеру. Так, до сфери безпеки життєдіяльності відноситься: забезпечення безпеки дорожнього руху; забезпечення безпечності та якості харчових продуктів та продовольчої сировини; забезпечення хімічної, біологічної та радіаційної безпеки; захист людини від техногенних факторів, які можуть завдати шкоди здоров'ю вдома чи на роботі (охорона праці), до яких можна віднести можливість ураження електричним струмом, небезпеку падіння з висоти, отруєння чадним газом, негативні наслідки від порушення правил роботи з хімічними реактивами та іншими небезпечними матеріалами (речовинами), наслідки порушення правил користування побутовими приборами та засобами виробництва (станками, інструментами та іншими знаряддями праці) тощо.

Значна частина правил забезпечення безпеки життєдіяльності міститься в технічних нормах, які представлені у формі інструкцій, правил користування приборами та технікою, правил поводження на певних об'єктах та з певними речовинами. До прикладу – це інструкції до побутової техніки, правила поведінки на воді, строки зберігання певних продуктів, вказані на упаковці тощо. Недотримання вказаних норм має наслідком негативні наслідки для здоров'я людини або становлять загрозу її життю.

Водночас в силу особливої важливості значна частина технічних норм закріплена в нормативно-правових актах. До прикладу – це Правила пожежної безпеки в Україні, затверджені наказом МВС України від 30.12.2014 № 1417 [237], Правила дорожнього руху, затверджені постановою Кабінету Міністрів

України від 10 жовтня 2001 р. № 1306 [272] та інші нормативні документи. В цих випадках технічні норми отримують юридичне оформлення та є вже техніко-юридичними нормами, за порушення яких встановлена адміністративна або кримінальна відповідальність, в залежності від наслідків їх порушення.

Водночас цивільний захист є більш вузьким поняттям, що включає захист людини, суспільства в цілому, а також навколишнього природного середовища від руйнівних негативних факторів (пожеж, землетрусів, повеней, цунамі, ураганів, епідемій, аварій на об'єктах критичної інфраструктури тощо), які призводять до виникнення надзвичайної ситуації, тобто ситуації, яка порушує нормальні умови життя і діяльності людей на об'єктах або територіях.

Науковці приділяють значну увагу питанням забезпечення безпеки життєдіяльності та цивільного захисту, формулюючи авторські визначення вказаних категорій.

Так, В. Кошель, Г. Сав'юк та Б. Дзундза визначають безпеку життєдіяльності як галузь знання та науково-практичну діяльність, що спрямовані на формування безпеки і попередження небезпеки шляхом вивчення загальних закономірностей виникнення небезпек, їхніх властивостей, наслідків їхнього впливу на організм людини, основ захисту здоров'я та життя людини і середовища її проживання від небезпек. Крім того, на думку вказаних науковців, безпека життєдіяльності – це інтегральна наука, що вивчає небезпеки та негативну дію на людину екзогенних та ендогенних факторів у всіх сферах життєдіяльності людини [153, с. 8].

Узагальнюючи вищезазначене, науковці зазначають, що безпека життєдіяльності – це наука, що вивчає проблеми безпечного перебування людини в середовищі – природному, техногенному, соціальному, в процесі різних видів її діяльності. Вона, на їх думку, є більш універсальною, ніж окремі напрямки наукових досліджень, такі як охорона праці чи цивільний захист, адже дві останні розглядають лише окремі випадки безпеки в конкретних

ситуаціях, зокрема охорона праці вивчає питання безпеки людини, яка знаходиться в умовах виробництва, а цивільний захист – в надзвичайних ситуаціях, тоді як безпека життєдіяльності – у всіх життєвих обставинах [153, с. 8].

Таким чином, безпека життєдіяльності – найбільш загальне поняття, що включає в себе і питання охорони праці, і питання цивільного захисту. Універсальність безпеки життєдіяльності як науки та навчальної дисципліни проявляється у тому, що вона охоплює майже всі сфери життєдіяльності людини, за виключенням хіба що особистого (інтимного) життя. Її по праву можна назвати науковою про правила та способи виживання людини в сучасному світі, адже незнання елементарних правил безпеки життєдіяльності може призвести до трагічних наслідків. Натомість цивільний захист працює (активується) лише у виключних випадках, пов'язаних із настанням надзвичайної ситуації, що спричинена природньою катастрофою або техногенною аварією, соціальним «вибухом» або розгортанням збройного конфлікту.

О. Арламов зазначає, що виходячи з сучасних уявлень, безпека життєдіяльності є багатогранним об'єктом розуміння і сприйняття дійсності, який потребує інтеграції різних стратегій, сфер, аспектів, форм і рівнів пізнання. Складовими цієї галузі є різноманітні науки про безпеку [12].

За визначенням, який наводить О. Арламов, безпека життєдіяльності – це галузь знання та науково-практична діяльність, спрямована на вивчення загальних закономірностей виникнення небезпек, їхніх властивостей, наслідків їхнього впливу на організм людини, основ захисту здоров'я та життя людини і середовища її проживання від небезпек, а також на розробку і реалізацію відповідних засобів та заходів щодо створення і підтримки здорових та безпечних умов життя і діяльності людини як у повсякденних умовах побуту та виробництва, так і в умовах надзвичайних ситуацій [12, с. 3].

Водночас, зазначає О. Арламов, під цивільним захистом розуміється «система організаційних, інженерно-технічних, санітарно-гігієнічних,

протиепідемічних та інших заходів, які здійснюються центральними і місцевими органами виконавчої влади, органами місцевого самоврядування, підпорядкованими їм силами і засобами, підприємствами, установами та організаціями незалежно від форми власності, добровільними рятувальними формуваннями, що забезпечують виконання цих заходів з метою запобігання та ліквідації надзвичайних ситуацій, які загрожують життю та здоров'ю людей, завдають матеріальних збитків у мирний час і в особливий період» [12, с. 79].

Наведене визначення достатньо повно відображає зміст поняття цивільного захисту, розкриваючи його інструментарій та окреслюючи коло суб'єктів, які здійснюють вказані заходи.

Крім того, О. Арламов наводить схематичне визначення цивільного захисту України як державної системи органів управління, сил та засобів, створеної для організації та забезпечення захисту населення від наслідків надзвичайних ситуацій техногенного, природного, соціально-політичного та воєнного характеру [12, с. 79].

Таке визначення найбільш точно та лаконічно відображає структуру національної системи цивільного захисту та характеризує види надзвичайних ситуацій.

На окрему увагу заслуговує нормативне визначення цивільного захисту. Так, у відповідності до ст. 4 Кодексу цивільного захисту України, цивільний захист – це комплекс заходів, які реалізуються на території України в мирний час та в особливий період і спрямовані на захист населення, територій, навколишнього природного середовища, майна, матеріальних і культурних цінностей від надзвичайних ситуацій та інших небезпечних подій, запобігання виникненню таких ситуацій та подій, ліквідацію їх наслідків, надання допомоги постраждалим, здійснення державного нагляду (контролю) у сфері пожежної та техногенної безпеки [143].

Таким чином, цивільний захист є складовою системи забезпечення безпеки життєдіяльності як більш широкого поняття. Безпека життєдіяльності

як наука розглядає всі засоби забезпечення безпеки людини у відносинах між людиною та природою, людиною та технічними засобами, а також у різноманітних суспільних відносинах, включаючи відносини із забезпечення пожежної, хімічної, біологічної, радіаційної безпеки, безпеки дорожнього руху, охорони праці, захисту територій та населення від надзвичайних ситуацій та їх наслідків тощо.

Водночас цивільний захист пов'язаний із захистом населення та територій від надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру, а також із ліквідацією наслідків надзвичайних ситуацій та мінімізацією їх негативного впливу на життя і здоров'я людей, навколишнє природне середовище тощо.

Отже, досліджуючи питання адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності неможливо оминути увагою і питання використання вказаних технологій в системі цивільного захисту України, що є складовою загальної системи забезпечення безпеки життєдіяльності населення України.

Проведений аналіз співвідношення понять безпеки життєдіяльності та цивільного захисту в контексті адміністративно-правового регулювання відповідних суспільних відносин дозволяє сформулювати висновок про те, що безпека життєдіяльності є найбільш загальною категорією, що характеризує суспільні відносини, пов'язані із захистом людини, населення в цілому та територій від різноманітних небезпек (впливу негативних факторів навколишнього природного середовища, техногенних небезпек, загроз від об'єктів підвищеної небезпеки, наслідків соціальних та воєнних конфліктів тощо) і включає в себе поняття цивільного захисту.

В свою чергу цивільний захист – це система заходів, спрямованих на захист життя та здоров'я людей, суспільства в цілому, а також територій, навколишнього природного середовища, об'єктів цивільної інфраструктури, матеріальних цінностей від чинників, які викликають надзвичайні ситуації, а

також наслідків надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру.

Окремо слід зазначити, що сучасний механізм забезпечення безпеки життєдіяльності та загальнодержавна система цивільного захисту функціонують в умовах інформаційного суспільства, коли поряд (паралельно) із оточуючим нас матеріальним світом існує віртуальний, цифровий світ, в якому наразі відбувається значна частина суспільних відносин і який містить чимало нових загроз безпеці життєдіяльності людини та суспільства в цілому. Крім того, цифровізація відкриває перед нами широкий спектр нових інноваційних засобів забезпечення безпеки життєдіяльності та цивільного захисту. Інноваційні інформаційні технології значно полегшують життя людей, а подекуди дозволяють повністю замінити людину, включаючи найбільш чутливі з точки зору забезпечення безпеки життєдіяльності сфери суспільних відносин (сфери виробництва та надання послуг з підвищеним ризиком для життя та здоров'я людини).

Таким чином безпеку життєдіяльності в контексті цифровізації доцільно визначити як комплексну науку та навчальну дисципліну, яка досліджує всі негативні чинники (небезпеки), які вливають або потенційно можуть вплинути на життєдіяльність людини в сучасному інформаційному суспільстві, порушити порядок нормального функціонування та розвитку суспільства в цілому, встановлює систему технічних та техніко-юридичних норм взаємодії людини із навколишнім середовищем та цифровим світом, а також визначає систему засобів запобігання та протидії вказаним негативним чинникам (небезпекам), ліквідації надзвичайних ситуацій та їх наслідків, включаючи інноваційні інформаційні технології, використання яких потребує належної адміністративно-правової регламентації.

Наведений підхід до нового розуміння безпеки життєдіяльності в контексті цифровізації обумовлює актуальність дослідження питань використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності (включаючи систему цивільного захисту), а також

адміністративно-правового регулювання відповідних суспільних відносин.

Враховуючи те, що діяльність органів публічної адміністрації у сфері забезпечення безпеки життєдіяльності та цивільного захисту повинна мати належну правову основу, важливо дослідити історію становлення та розвитку адміністративно-правового регулювання вказаних суспільних відносин.

1.3 Історія становлення та розвитку адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності

Дослідження актуальних питань адміністративно-правового регулювання у сферах забезпечення безпеки життєдіяльності та цивільного захисту в контексті цифровізації обов'язково має включати аналіз історії становлення відповідних інституцій, розвитку системи органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, а також тенденцій щодо цифровізації суспільних відносин.

Вивчення історії є необхідним для урахування всіх позитивних аспектів та можливих прорахунків в реформуванні відповідних органів публічної адміністрації, визначення актуальних напрямів удосконалення адміністративно-правового регулювання у сферах забезпечення безпеки життєдіяльності та цивільного захисту з урахуванням дослідженого історичного досвіду.

Становлення та розвиток системи органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, включає декілька ключових етапів.

Основну увагу доцільно зосередити на дослідженні новітньої історії становлення та розвитку органів публічної адміністрації у сфері забезпечення безпеки життєдіяльності та цивільного захисту, адже на перших етапах формування національної державності функціонувала радянська система цивільного захисту, яку успадкувала молода українська держава.

Після здобуття Україною незалежності в 1991 році, питаннями

цивільного захисту та оборони, ліквідації наслідків та попередження надзвичайних ситуацій, захисту населення від наслідків Чорнобильської катастрофи, гасіння пожеж та пожежної безпеки займалися три окремих відомства: Штаб Цивільної оборони; Міністерство у справах захисту населення від наслідків аварії на ЧАЕС; Головне управління пожежної охорони МВС України [94, с. 4].

Як видно з самих назв вищевказаних органів публічної адміністрації, які реалізовували державну політику у сфері цивільного захисту, пріоритет надавався питанням ліквідації аварії на Чорнобильській атомній електростанції, що було обумовлено масштабами вказаної техногенної катастрофи, яка має міжнародний характер і досі залишається актуальною проблемою для всього людства. В контексті теми даного дослідження слід відзначити, що причиною цієї аварії став людський фактор, а саме, ручне управління вкрай небезпечними процесами на ядерному реакторі. Цей страшний урок історії вказує на необхідність використання автоматизованих систем, інформаційних технологій для управління складними технологічними процесами з метою запобігання неконтрольованому втручанню людини у вказані процеси та забезпечення автоматичного блокування та нормалізації роботи відповідних технологічних систем у разі загрози життю та здоров'ю людей або навколишньому природному середовищу.

У 1996 році Указом Президента Л. Кучми на базі Штабу Цивільної оборони та Мінчорнобиля було створено єдине відомство – Міністерство з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи (МНС України) [94, с. 4].

Це нове відомство стало провідним органом у системі виконавчої влади із забезпечення реалізації державної політики у сфері цивільної оборони, рятувальної справи, створення та функціонування систем страхового фонду документації, поводження з радіоактивними відходами, захисту від надзвичайних ситуацій, попередження ситуацій і реагування на них, ліквідації їх наслідків та наслідків Чорнобильської катастрофи [94, с. 4].

Міністерство з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи здійснювало керівництво дорученою йому сферою управління та несло відповідальність за її стан і розвиток. В його підпорядкуванні перебували угрупування військ Цивільної оборони чисельністю 10 218 осіб, з них 9550 – військовослужбовці. Війська ЦО були призначені для захисту населення і територій у разі виникнення надзвичайних ситуацій [94, с. 4].

Таким чином, система органів публічної адміністрації у сфері цивільного захисту до 2003 року мала в підпорядкуванні достатньо потужне угрупування військ Цивільної оборони, яке було нерівномірно розподілене за територіальним принципом та свідчило про рудименти радянського (мілітаристського) підходу до організації цивільного захисту (який розглядався більшою мірою як елемент підготовки до потенційної ядерної війни та застосування хімічної чи біологічної зброї західними державами).

Територіальні органи МНС України до 2003 року були представлені Головними управліннями (управліннями) з питань надзвичайних ситуацій (у складі обласних державних адміністрацій).

27 січня 2003 року Указом Президента України «Про заходи щодо вдосконалення державного управління у сфері пожежної безпеки, захисту населення і територій від наслідків надзвичайних ситуацій» органи і підрозділи Державної пожежної охорони виведені зі складу МВС і передані до складу МНС України [94, с. 5].

Слід відзначити, що належність підрозділів Державної пожежної охорони до складу МВС не відповідала правовій природі органу публічної адміністрації, який реалізує державну політику у сфері правоохоронної діяльності.

Важливим етапом в розвитку органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, стала демілітаризація підрозділів цивільної оборони.

Так, 19 грудня 2003 року було видано Указ Президента України «Про

Державну програму перетворення військ Цивільної оборони України, органів і підрозділів державної пожежної охорони в оперативно-рятувальну службу цивільного захисту на період до 2005 року».

Державна програма передбачала створення єдиної невійськової Оперативно-рятувальної служби. Передбачалася повна демілітаризація МНС. Військові частини Військ Цивільної оборони були розформовані або реорганізовані в рятувальні загони Оперативно-рятувальної служби, або увійшли до кладу аварійно-рятувальних загонів спеціального призначення [94, с. 5].

Слід відзначити, що демілітаризація органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, відповідає загальноєвропейським стандартам та світовій практиці, коли військові підрозділи залучаються до ліквідації надзвичайних ситуацій лише у крайніх випадках, у випадку масштабних природніх або техногенних катастроф із наслідками, які охоплюють декілька регіонів, поширюються на територію всієї держави, або мають міждержавний характер.

Після реформи 2003 року були сформовані нові територіальні органи МНС – Головні управління (управління) МНС України на базі Управлінь пожежної безпеки ГУ (У) МВС України у регіонах [94, с. 5].

Таким чином, відбулось формування регіональних підрозділів Міністерства з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, що стало важливим кроком на шляху створення сучасної єдиної державної системи цивільного захисту.

У 2005 році був прийнятий Закон України «Про правові засади цивільного захисту», що визначав правові та організаційні засади у сфері цивільного захисту населення і територій від надзвичайних ситуацій, повноваження виконавчої влади та органів управління, порядок створення і застосування сил, їх комплектування, проходження служби, а також гарантії соціального і правового захисту особового складу органів і підрозділів цивільного захисту [94, с. 5].

Належна правова регламентація суспільних відносин у сфері цивільного захисту сприяла удосконаленню публічного управління у вказаній сфері суспільних відносин та створювала мотиваційні засади для кадрового забезпечення структурних підрозділів органів публічної адміністрації, які реалізовували державну політку у сфері цивільного захисту на той час.

У 2006 році війська цивільної оборони України були повністю розформовані, особовий склад військ і Державної пожежної охорони влився в ряди єдиної Оперативно-рятувальної служби цивільного захисту МНС України. У 2008 році була запроваджена контрактна служба, проведена переатестація в спеціальні звання служби цивільного захисту [94, с. 5].

Слід відзначити, що запровадження контрактної служби в органах публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, сприяло удосконаленню кадрового складу Оперативно-рятувальної служби цивільного захисту МНС України, залученню до роботи в службі висококваліфікованих працівників, включаючи фахівців у сфері розвитку та впровадженні інноваційних інформаційних технологій.

У грудні 2010 року Міністерство з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи було реорганізовано в Міністерство надзвичайних ситуацій України. Державний пожежний та техногенний нагляд, управління зоною відчуження та ЧАЕС, Держгіртехнагляд стали центральними органами виконавчої влади [94, с. 6].

Така реорганізація була проведена в рамках загальної адміністративної реформи у відповідності до Указу Президента України «Про оптимізацію системи центральних органів виконавчої влади» від 9 грудня 2010 року № 1085/2010. Так, у відповідності до вказаного Указу, утворено Міністерство надзвичайних ситуацій України, Державну службу гірничого нагляду та промислової безпеки України, Державне агентство України з управління зоною відчуження, Державну інспекцію техногенної безпеки України, шляхом реорганізації Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи.

Таким чином, у 2011 році сталося розділення Міністерства надзвичайних ситуацій України на чотири окремих відомства – Міністерство надзвичайних ситуацій України (як головний орган), Державну інспекцію техногенної безпеки, Державне агентство зони відчуження та Державну службу гірничого нагляду та промислової безпеки [94, с. 6-7].

Особовий склад залишився на службі цивільного захисту. Державні пожежні частини отримали статус «рятувальних» і були підпорядковані територіальним органам МНС. Районні (міські) відділи МНС реформовані в служби цивільного захисту в районах (містах) і введені до складу апаратів ГТУ (ТУ) МНС [94, с. 7].

24 грудня 2012 року у відповідності до Указу Президента України «Про деякі заходи з оптимізації системи центральних органів виконавчої влади» № 726/2012 Міністерство надзвичайних ситуацій та Державна інспекція техногенної безпеки України були реорганізовані в єдину Державну службу України з надзвичайних ситуацій. У відповідності до вказаного Указу, ДСНС України було визначено як центральний орган виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через відповідного члена Кабінету Міністрів України, а саме – через Міністра оборони України. Відповідно, було затверджено Положення про Державну службу України з надзвичайних ситуацій, сформовані відповідні управління ДСНС.

Слід відзначити, що не зважаючи на важливість забезпечення безпеки життєдільності та цивільного захисту населення та територій від надзвичайних ситуацій, доцільно, щоб орган публічної адміністрації, який реалізує державну політику у сфері цивільного захисту, був представлений саме у формі державної служби, адже будь-яке міністерство за своїм статусом є більшою мірою політичним органом, який формує державну політику у певній сфері суспільних відносин. Наприклад, є Міністерство внутрішніх справ України і є Національна поліція, є Міністерство оборони і є Національна гвардія. Водночас державна служба за своїм статусом більшою мірою наближена до

реальних суспільних відносин, здійснює їх адміністрування та публічне управління в цілому.

1 липня 2013 року набув чинності Кодекс цивільного захисту України, у відповідності до якого Оперативно-рятувальна служба цивільного захисту – спеціальне невійськове об'єднання аварійно-рятувальних та інших формувань, органів управління такими формуваннями системи центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері цивільного захисту [94, с. 7].

Згідно із чинним Положенням про Державну службу України з надзвичайних ситуацій (затверджене Постановою КМУ від 16 грудня 2015 р. № 1052 (з наступними змінами) 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 [246].

Підпорядкування Державної служби України з надзвичайних ситуацій саме Міністерству внутрішніх справ є цілком логічним, адже саме МВС є головним органом у системі центральних органів виконавчої влади, що забезпечує формування державної політики, у тому числі, і у сфері цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб.

В мирний час діяльність ДСНС України спрямована більшою мірою на цивільний захисту населення та територій від надзвичайних ситуацій природного та техногенного характеру.

Водночас на окрему увагу в контексті історії заслуговує питання особливостей роботи Державної служби України з надзвичайних ситуацій в умовах воєнного стану.

Науковці зазначають, після підписання Президентом України 24 лютого 2022 року Указу № 64/2022 «Про введення воєнного стану в Україні» система цивільного захисту України повинна була працювати у нових реаліях. Небезпечні умови роботи рятувальників вимагали нових, особливих підходів до вирішення проблем по забезпеченню цивільного захисту в період воєнного стану. Головне завдання – безпека самих рятувальників при виїзді на виклики, під час гасіння пожеж на об'єктах критичної інфраструктури. В зону воєнних дій потрапили хімічно небезпечні об'єкти та об'єкти, де знаходяться радіоактивні речовини. Крім того, суттєво підвищилась потенційна загроза використання хімічної або ядерної зброї. Звичайно, вся територія бойових дій, а це – сотні тисяч квадратних кілометрів, піддалась забрудненню різноманітними вибухонебезпечними предметами. І основною роботою на звільнених територіях є саме розмінування та видалення вибухонебезпечних предметів. Потужні удари ворога по об'єктах енергетики призвели до масштабних блекаутів по всій території країни, з наслідками від яких постійно доводиться боротися [195, с. 11].

Таким чином, органи публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, в умовах правового режиму воєнного стану перейшли у стан фактично цілодобової підвищеної готовності до реагування на надзвичайні події та ситуації.

Н. Клименко також зазначає, що Єдина державна система цивільного захисту з 24 лютого 2022 року функціонувала одночасно у двох режимах: режимі надзвичайної ситуації, встановленому з метою ліквідації наслідків медико-біологічної надзвичайної ситуації природного характеру державного рівня і забезпечення санітарного й епідемічного благополуччя населення, та перебувала у готовності до виконання завдань за призначенням в особливий період, у тому числі у воєнний час, з урахуванням особливостей, що

визначаються згідно з нормами міжнародного гуманітарного права, законами України «Про правовий режим воєнного стану» [274] та «Про мобілізаційну підготовку та мобілізацію» [266]. На її територіальні та функціональні підсистеми й сили цивільного захисту покладалася ліквідація наслідків надзвичайних ситуацій, які відбувалися не тільки в повсякденних умовах, в умовах режиму надзвичайної ситуації та карантину, а й під час воєнного стану [136, с. 227].

Таким чином, адміністративно-правове регулювання діяльності органів публічної адміністрації у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану здійснюється з урахуванням вимог спеціальних законів, якими врегульовано правовий режим воєнного стану та порядок проведення мобілізаційної підготовки та мобілізації.

Окремої уваги заслуговує також питання історії цифровізації системи органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту. Сучасні інформаційні технології здатні суттєво змінити підходи до здійснення публічного управління у сфері цивільного захисту, оптимізувати процеси аналізу та обміну інформацією, удосконалити механізми мобілізації сил та засобів цивільного захисту, а також залучення добровольців з метою оперативної ліквідації надзвичайних ситуацій та їх наслідків.

Науковці виділяють кілька етапів у еволюції цифрових технологій України [172; 71, с. 157].

Так, для першого етапу (1990-2000 рр.), на їх думку, характерним є формування інфраструктури з метою широкого доступу до Інтернету, використання отриманої інформації для ознайомлення, а не для комунікації чи ведення бізнесу. У цей період в 1998 році був прийнятий Закон України «Про Національну програму інформатизації». У вказаному законі було визначено напрямки вирішення питань щодо забезпечення інформаційних потреб у загальнодержавній, економічній, науково-технічній, екологічній та національно-культурній діяльності. Програма була спрямована на

вдосконалення інформаційної інфраструктури України, тобто здійснення комплексу заходів з метою впровадження досягнень у сфері інформатизації в державне управління та оборону країни, національну безпеку, економіку, освіту й науку, охорону довкілля та культуру.

На цьому етапі відбувалось фактичне забезпечення органів публічної адміністрації комп'ютерною технікою, підключення їх до інтернету, навчання державних службовців засадам комп'ютерної грамотності. У сфері цивільного захисту комп'ютеризація та використання Інтернет дозволили вийти на новий рівень комунікації між підрозділами Міністерства з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи та Головними управліннями (управліннями) з питань надзвичайних ситуацій у складі обласних державних адміністрацій.

Наступний (другий) етап (2000-2010 рр.) – це період, коли користувачі Інтернету перейшли від пасивного споглядання до створення та захисту інформаційних електронних ресурсів, упровадження електронного документообігу. Цей період характеризувався наявністю значного кадрового потенціалу у сфері інформаційно-комп'ютерних технологій, швидкими темпами оновлення комп'ютерної техніки, високим рівнем інформатизації банківської діяльності. Проте недостатніми залишалися підтримка з боку держави щодо виробництва та впровадження інформаційних засобів та інформаційно-комп'ютерних технологій, розвиток нормативної бази щодо інформатизації суспільства, створення інфраструктури з метою надання інформаційних послуг органам державної влади, місцевого самоврядування, населенню [71, с. 157].

На вирішення зазначених вище проблем у 2007 році прийнято Закон «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Було виокремлено такі стратегічні цілі: вдосконалення державного управління та місцевого самоврядування шляхом розроблення та широкого впровадження інформаційно-комп'ютерних технологій; зростання інформаційної грамотності громадян та захист їхніх інформаційних прав;

інтеграція вітчизняної та світової інформаційної інфраструктури, розширення асортименту «електронних» послуг у сферах освіти та науки, охорони здоров'я та довкілля, культури та соціального захисту. Статистичні дані свідчать, що реалізація стратегічних цілей цього закону сприяла розвитку людського потенціалу, підвищенню конкурентоспроможності економіки та становленню демократичного суспільства [71, с. 157].

Таким чином, на другому етапі завершився процес комп'ютеризації системи органів публічної адміністрації, електронний документообіг отримав належну правову основу у вигляді Закону України «Про електронні документи та електронний документообіг», який було прийнято у 2003му році. Цей період збігся із процесами демілітаризації підрозділів цивільної оборони та створенням якісно нової системи органів публічної адміністрації у сфері цивільного захисту. Впровадження інформаційних технологій, електронного документообігу дозволило суттєво удосконалити організацію публічного управління у сфері пожежної безпеки, захисту населення і територій від наслідків надзвичайних ситуацій.

Третій етап (2010-2020 рр.) характеризувався впровадженням електронного урядування та наданням публічних електронних послуг. Проте на початку цього етапу розбудова інформаційного суспільства в Україні не відповідала потребам та можливостям країни, відбувалося гальмування розвитку інформаційної сфери. З метою усунення вищезгаданих недоліків у 2013 році Кабінет Міністрів України видав розпорядження «Про схвалення стратегії розвитку інформаційного суспільства в Україні». Документ був спрямований на удосконалення нормативних засад з метою розвитку інформаційної сфери, впровадження інструментів е-демократії та електронного урядування, здійснення заходів з метою розвитку електронної економіки, покращення інформаційної грамотності громадян, підвищення рівня якості адміністративних послуг і стану інформаційної безпеки [71, с. 158].

У 2014 році створено Державне агентство з питань електронного

урядування, завданнями якого було впровадження політики Уряду країни з метою розвитку інформаційного суспільства, використання електронних інформаційних ресурсів, ширшого впровадження електронних послуг та сервісів, цифровізації центральних та місцевих органів влади.

Першочергові завдання та проекти «цифровізації» України до 2020 року були викладені у документі «Цифрова адженда України-2020», який розроблений у 2016 році представниками Міністерства економічного розвитку й торгівлі України, Державного агентства з питань електронного урядування, компаній-лідерів світового цифрового ринку, громадських організацій, асоціацій та консалтингових компаній. Автори виділили стратегічні цілі, підходи до впровадження та інструменти для стимулювання розвитку цифровізації в наступних сферах: економіка, державне управління, освіта, національна кібербезпека, суспільно-економічна діяльність (охорона здоров'я, наука, соціальна сфера, електронна демократія, електронне урядування, електронна комерція, електронні платежі) [71, с. 158].

Базуючись на проекті цифровізації країни, прийнятому у 2016 році, у січні 2018 року Кабінет Міністрів ухвалив «Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки». Передбачався розвиток цифрової інфраструктури, цифрових навичок громадян, цифрові трансформації в забезпеченні громадської безпеки, охорони навколишнього природного середовища, життєдіяльності міст, гармонізації з європейськими та світовими науковими ініціативами [71, с. 159].

Предметом відання Комітету Верховної Ради України з питань цифрової трансформації, утвореному в серпні 2019 року, стали законодавчі засади цифровізації країни та використання мережі Інтернет, державні програми інформатизації та програми цифрового європейського співробітництва, нововведення в сфері цифрового підприємництва, цифрові телекомунікації, смарт інфраструктура, кібербезпека і кіберзахист, розвиток сфери «відкритих даних» та цифрових компетентностей.

У вересні 2019 року Кабінет Міністрів України створив Міністерство цифрової трансформації України на основі реорганізації Державного агентства з питань електронного урядування. До функцій цього органу публічної адміністрації віднесено: формування та реалізація державної політики у сфері розвитку інформаційного суспільства, цифрової економіки, електронного урядування та електронної демократії, надання електронних та адміністративних послуг, впровадження електронного документообігу, розвитку робототехніки та технології штучного інтелекту, інших цифрових інновацій, ІТ-індустрії тощо [71, с. 159].

Таким чином, третій етап характеризувався високими темпами діджиталізації публічного управління та активним реформування органів публічної адміністрації, які реалізують державну політику у сфері цифровізації, впровадження інформаційних технологій з метою поступового перетворення усіх державних послуг на зручні онлайн-сервіси. Новостворена Державна служба України з надзвичайних ситуацій також була залучена до процесів розвитку електронного урядування, удосконалення інтерфейсу та наповнення офіційних веб-сайтів органів публічної адміністрації, надання цифрових адміністративних послуг тощо.

Четвертий етап, який умовно розпочався у 2020 році, характеризується використанням штучного інтелекту, хмарних технологій, дронів, коботів, Інтернету речей та послуг, опрацюванням великих масивів даних, застосуванням систем «розумне місто» та «розумне підприємство» [71, с. 159].

Значні досягнення в цифровій трансформації та розвитку електронного урядування відбуваються завдяки долученню України у вересні 2022 року до Програми «Цифрова Європа» на період до 2027 року. Протягом семи років 6 млрд. євро будуть виділені Україні на фінансування проектів за такими напрямками: штучний інтелект, дані та хмарні послуги; цифрові технології в бізнесі та суспільстві; цифрові навички [71, с. 160].

Таким чином, четвертий етап, який наразі триває, характеризується революційними процесами у сфері використання інноваційних інформаційних

технологій, серед яких ключовою є технологія штучного інтелекту. Остання здатна замінити людину у багатьох сферах виробництва та надання послуг, а також у сфері публічного управління, адміністрування суспільних відносин, включаючи суспільні відносини у сферах забезпечення безпеки життєдіяльності та цивільного захисту. Не менш важливими є процеси глобалізації, які для України відбуваються у формі євроінтеграції, адаптації національного законодавства до права ЄС, включаючи інформаційне право.

Щодо цифровізації діяльності органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, та правової регламентації впровадження інноваційних інформаційних технологій у вказану сферу суспільних відносин, в історичному аспекті слід відзначити наказ МВС України від 04.05.2016 № 356 «Про затвердження Положення про підсистему реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт єдиної державної системи цивільного захисту» [186] та наказ МВС України від 20.04.2023 № 326 «Про затвердження Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ» [255].

Так, у відповідності до Положення про підсистему реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт єдиної державної системи цивільного захисту, підсистема реагування на надзвичайні ситуації утворюється ДСНС з метою організації та здійснення робіт, спрямованих на ліквідацію або мінімізацію наслідків надзвичайної ситуації, локалізацію її зони, припинення дії або впливу небезпечних факторів, викликаних надзвичайною ситуацією, пошук, рятування і захист населення, майна, а також ліквідацію чинників, що унеможливлюють проведення таких робіт або загрожують життю рятувальників.

Завданнями Підсистеми реагування на надзвичайні ситуації є: забезпечення готовності органів управління, сил і засобів Оперативно-

рятувальної служби цивільного захисту до дій, спрямованих на запобігання виникненню та реагування на надзвичайні ситуації і небезпечні події; організація та проведення моніторингу і прогнозування виникнення надзвичайних ситуацій та їх розвитку, визначення ризику виникнення надзвичайних ситуацій; організація та проведення робіт щодо рятування людей, надання допомоги у ліквідації наслідків аварій, катастроф, стихійного лиха та інших видів небезпечних подій, що становлять загрозу життю або здоров'ю населення чи призводять до завдання матеріальних збитків, та гасіння пожеж; залучення органів управління та формувань Оперативно-рятувальної служби цивільного захисту до ліквідації наслідків надзвичайних ситуацій державного і регіонального рівнів та координація їх діяльності під час проведення аварійно-рятувальних та інших невідкладних робіт; своєчасне і достовірне інформування заінтересованих центральних і місцевих органів виконавчої влади про загрозу виникнення або виникнення надзвичайних ситуацій; забезпечення планування заходів цивільного захисту; здійснення заходів цивільного захисту відповідно до компетенції ДСНС; виконання піротехнічних робіт відповідно до компетенції ДСНС, а також проведення робіт із гуманітарного розмінування; здійснення заходів з мінімізації та ліквідації наслідків надзвичайних ситуацій, пов'язаних із технологічними терористичними проявами та іншими видами терористичної діяльності під час проведення антитерористичних операцій; розроблення та забезпечення виконання планів реагування на надзвичайні ситуації; раціональне використання оперативного матеріального резерву для оперативного реагування на надзвичайні ситуації; контроль за готовністю авіаційних сил та засобів пошуку і рятування, управління діяльністю координаційних центрів з пошуку і рятування в єдиній системі проведення авіаційних робіт з пошуку і рятування, координація проведення аварійно-рятувальних та інших невідкладних робіт авіаційними силами і засобами ДСНС; проведення навчань (тренування) органів управління функціональної підсистеми та

підпорядкованих їй сил цивільного захисту згідно з планом основних заходів цивільного захисту ДСНС на відповідний рік [254].

Крім того, у відповідності до Положення про підсистему реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт єдиної державної системи цивільного захисту, до складу Підсистеми реагування на надзвичайні ситуації входять: у режимах повсякденного функціонування, підвищеної готовності та надзвичайної ситуації – орган управління Підсистемою реагування на надзвичайні ситуації (апарат ДСНС); органи управління та формування Оперативно-рятувальної служби цивільного захисту; у режимі надзвичайного стану та в особливий період, у разі проведення мобілізації – орган управління Підсистемою реагування; органи управління та формування Оперативно-рятувальної служби цивільного захисту; спеціальні формування, призначені для виконання окремих завдань цивільного захисту міст, віднесених до груп цивільного захисту, та суб'єктів господарювання, віднесених до категорій цивільного захисту [254].

Також у відповідності до вказаного Положення, до сил Підсистеми реагування на надзвичайні ситуації належать формування Оперативно-рятувальної служби цивільного захисту, які залучаються до виконання аварійно-рятувальних та інших невідкладних робіт, а також спеціальні формування в режимі надзвичайного стану та в особливий період. Безпосереднє керівництво Підсистемою реагування на надзвичайні ситуації здійснюється Головою ДСНС. Управління Підсистемою реагування на надзвичайні ситуації здійснюють: на державному рівні – Голова ДСНС; на регіональному рівні – керівники територіальних органів ДСНС. Для управління у режимі повсякденного функціонування суб'єктами забезпечення цивільного захисту, координації дій органів управління та сил цивільного захисту, здійснення цілодобового чергування та забезпечення функціонування системи збору, оброблення, узагальнення та аналізу інформації про обстановку в районах надзвичайних ситуацій у системі ДСНС функціонують:

на державному рівні – Державний центр управління в надзвичайних ситуаціях; на регіональному рівні – центри управління в надзвичайних ситуаціях [254].

Таким чином, в Україні протягом відносно незначного періоду історії незалежної держави було створено розгалужену систему органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту на чолі з Державною службою України з питань надзвичайних ситуацій, діяльність якої спрямовується та координується Міністерством внутрішніх справ України. Отже, використання інформаційних технологій у сфері забезпечення життєдіяльності та цивільного захисту здійснюється на основі нормативних документів, розроблених та затверджених МВС України.

В свою чергу, у відповідності до Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ, СУСЗ (система управління силами та засобами) – це інтегрована інформаційно-комунікаційна система, що забезпечує збирання, зберігання, використання, передачу, захист інформації про сили та засоби цивільного захисту, об’єкти, на яких існує загроза виникнення надзвичайних ситуацій, пожеж та інших небезпечних подій, у тому числі об’єкти підвищеної небезпеки, надзвичайні ситуації, небезпечні події, у тому числі пожежі, а також іншої інформації, необхідної для керування силами та засобами цивільного захисту, а також оперативно-диспетчерського управління ними [255].

Враховуючи особливу важливість та актуальність питань забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану, доцільно розробити та впровадити в практичну діяльність самостійну інформаційну (автоматизовану) систему цивільного захисту з інтегрованою інтерактивною картою надзвичайних ситуацій та подій, які відбувались та відбуваються на території України, інтерактивною картою укриттів (захисних споруд) для населення на час повітряної тривоги з можливістю побудови маршруту до них з урахуванням геолокації (місцезнаходження) користувача, а також інформаційною базою добровольців з використанням спеціального

мобільного застосунку «Я доброволець», що дозволить оперативно мобілізувати бажаючих прийняти участь в ліквідації надзвичайної ситуації та її наслідків (з урахуванням місцезнаходження або проживання добровольців, які встановили вказаний мобільний застосунок та за власною згодою додані до бази добровольців). При розробці вказаної інформаційної системи варто використовувати технологію штучного інтелекту, алгоритми якого дозволять здійснювати оперативний аналіз інформації про надзвичайні події та їх наслідки, генерувати поради щодо вирішення актуальних питань цивільного захисту, а також здійснювати прогнозування виникнення надзвичайних ситуацій у майбутньому шляхом системного аналізу всіх кліматичних, географічних, демографічних, економічних, соціальних та інших чинників.

Висновки до розділу 1

1. Історіографія дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності об’єднує чотири групи наукових літературних джерел.

Так, до першої групи слід віднести підручники, навчальні посібники, монографії, публікації у періодичних виданнях, присвячені питанням забезпечення безпеки життєдіяльності, підготовлені фахівцями з прикладних, технічних та природничих наук.

До другої групи слід віднести наукові видання, монографії, дисертаційні дослідження, присвячені питанням використання інформаційних технологій у різних сферах суспільних відносин, включаючи основні напрями та способи цифровізації, використання цифрових інструментів для досягнення публічних та приватних цілей учасників суспільних відносин, надання цифрових послуг тощо.

До третьої групи слід віднести дослідження, присвячені адміністративно-правовому регулюванню інформаційних відносин, включаючи адміністративно-правові засади інформатизації, використання

цифрових інструментів, надання цифрових адміністративних послуг, а також правове регулювання порядку збирання, зберігання та використання інформації в комп'ютерних мережах, питання відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, правове регулювання Інтернет, технології штучного інтелекту та інших інформаційних технологій.

До четвертої групи слід віднести дослідження науковців, присвячені організації публічного управління та правовому регулюванню у сфері забезпечення безпеки життєдіяльності.

2. Аналіз методології дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволив сформулювати висновок про необхідність органічного поєднання в процесі наукового пошуку законів, прийомів та принципів діалектики, основних загальнонаукових та спеціально-юридичних методів дослідження, а також доцільність використання провідних наукових підходів: цивілізаційного, телеологічного та синергетичного.

Телеологічний підхід, зокрема, передбачає, що метою будь-якого дослідження у сфері права повинна бути практично значима мета, наприклад, розробка конкретних пропозицій щодо внесення змін до чинного законодавства або прийняття перспективних нормативно-правових актів. Отже, дана публікація є теоретико-методологічною основою для дослідження актуальних питань адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності з метою формулювання раціональних пропозицій щодо удосконалення національного адміністративного законодавства та юридичної практики у вказаній сфері суспільних відносин.

3. Проведене дослідження історії становлення та розвитку органів публічної адміністрації у сфері забезпечення безпеки життєдіяльності та цивільного захисту в контексті адміністративно-правового регулювання та

цифровізації їх діяльності дозволяє сформулювати висновок про те, що в Україні відбувся ряд реформ органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, включаючи демілітаризацію військ цивільної оборони, що в результаті призвело до утворення нині діючої Державної служби України з надзвичайних ситуацій, діяльність якої спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ.

В історії цифровізації діяльності органів публічної адміністрації, включаючи впровадження інформаційних технологій в діяльність Державної служби України з надзвичайних ситуацій, можна умовно виділити чотири основних етапи, останній з яких характеризується активним впровадженням інноваційних інформаційних технологій у сферу забезпечення безпеки життєдіяльності та цивільного захисту, що включає: використання технології штучного інтелекту та можливостей мобільних застосунків, створення автоматизованих інтегрованих інформаційних систем цивільного захисту тощо.

З урахуванням дослідженого історичного досвіду пропонується розробити та впровадити в практичну діяльність ДСНС окрему інформаційну систему цивільного захисту з інтегрованою інтерактивною картою надзвичайних ситуацій та подій, які відбувались та відбуваються на території України, інтерактивною картою укриттів (захисних споруд) для населення на час повітряної тривоги з можливістю побудови маршруту до них з урахуванням геолокації користувача, а також інформаційною базою добровольців з використанням спеціального мобільного застосунку «Я доброволець», що дозволить оперативно мобілізувати бажаючих прийняти участь в ліквідації актуальної надзвичайної ситуації та її наслідків.

РОЗДІЛ 2
СУЧАСНИЙ СТАН АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

2.1 Адміністративно-правові засади побудови системи цивільного захисту та забезпечення безпеки життєдіяльності в Україні

Порядок функціонування національних систем забезпечення безпеки життєдіяльності та цивільного захисту врегульовано ієрархією нормативно-правових актів, включаючи Конституцію України, ратифіковані міжнародні договори, кодекси та закони України, укази Президента України та постанови Кабінету Міністрів України, накази органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, спільні накази органів публічної адміністрації з питань цивільного захисту та безпеки життєдіяльності в різних сферах суспільних відносин, акти органів місцевого самоврядування, а також судову практику, зокрема, правові позиції (висновки) Верховного Суду та касаційних судів у складі Верховного Суду.

Так, у відповідності до ст. 50 Конституції України, «Кожен має право на безпечне для життя і здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди. Кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. Така інформація ніким не може бути засекречена» [149].

Також слід зазначити, що національне законодавство знаходиться в процесі кардинальної трансформації, зумовленої необхідністю приведення його у відповідність до норм та принципів права Європейського Союзу, а також продовженням процесів цифровізації суспільних відносин.

Ключовим документом, яким врегульовано питання адаптації національного законодавства до права ЄС є Угода про асоціацію між

Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [317].

Главою 6 «Навколишнє природне середовище» розділу 5 «Економічне і галузеве співробітництво» Угоди про асоціацію між Україною та Європейським Союзом передбачено співробітництво у сфері цивільного захисту.

Так, у відповідності до ст. 364 Угоди, співробітництво у сфері цивільного захисту здійснюється шляхом імплементації окремих угод в цій галузі, укладених між Сторонами згідно з відповідними владними повноваженнями та компетенцією ЄС і його держав-членів та відповідно до правових процедур кожної зі Сторін. Воно, зокрема, буде спрямоване на: сприяння взаємній допомозі у випадках надзвичайних ситуацій; цілодобовий обмін найостаннішими повідомленнями і оновленою інформацією про транскордонні надзвичайні ситуації, зокрема запити та пропозиції щодо допомоги; оцінку впливу наслідків надзвичайних ситуацій на навколишнє середовище; залучення експертів до участі у специфічних технічних семінарах та симпозіумах з питань цивільного захисту; залучення, у разі необхідності, спостерігачів під час проведення окремих навчань і тренінгів, що організовуються Україною та/або ЄС; посилення існуючого співробітництва щодо найефективнішого використання наявних можливостей цивільного захисту [317].

Згідно з даними офіційного веб-сайту, ДСНС України здійснює співробітництво з Європейським Союзом за наступними напрямами:

- реалізація положень Адміністративної домовленості між МНС України та Генеральним Директоратом «Навколишнє середовище» Європейської Комісії щодо співпраці між Центром моніторингу та інформації Механізму цивільного захисту співтовариства та Оперативно-черговою службою МНС України;

- у рамках інструменту ЄС «Східне Партнерство»;

- реалізація Порядку денного асоціації Україна – ЄС;

- виконання Першочергових заходів щодо інтеграції України до ЄС;

- Комітет з питань співробітництва між Україною та ЄС [103].

Відповідно до Адміністративної домовленості між МНС України та Генеральним Директоратом «Навколишнє середовище» Європейської Комісії щодо співпраці між Центром моніторингу та інформації Механізму цивільного захисту співтовариства та Оперативно-черговою службою МНС України, сторони взяли на себе зобов'язання щодо сприяння взаємній допомозі у випадках надзвичайних ситуацій, спільної роботи з оцінювання впливу наслідків стихійного лиха на навколишнє середовище, залучення експертів до участі у профільних технічних семінарах, співробітництва у галузі більш ефективного використання існуючих сил та засобів цивільного захисту, цілодобового обміну інформацією з Координаційним центром реагування на надзвичайні ситуації Механізму цивільного захисту щодо надзвичайних ситуацій техногенного та природного характеру, що виникли на території країн-членів ЄС та інших держав світу [103].

Державна служба України з надзвичайних ситуацій у рамках Угоди про асоціацію між Україною та ЄС виконує в межах повноважень завдання визначені Главою 6 «Навколишнє природне середовище» Розділу V «Економічне та галузеве співробітництво» Плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, відповідно до постанови Кабінету Міністрів України від 25 жовтня 2017 року № 1106 [63.

Крім того, ДСНС України є основним бенефіціаром Проєкту ЄС «Програма з попередження, готовності та реагування на катастрофи природного та техногенного характеру для країн Східного партнерства». Метою зазначеної Програми є посилення і розвиток потенціалу країн-учасниць Східного партнерства у сфері цивільного захисту шляхом залучення експертної та технічної підтримки ЄС [63].

Вказана Програма спрямована на розвиток національного інституційного та регуляторного правового поля з наголосом на політиці цивільного захисту Європейського союзу та Директиві ЄС з питань запобігання і реагування на повені. Заходи з підвищення потенціалу орієнтовані на підготовку країн-партнерів до відкриття Європейського Механізму цивільного захисту Європейського Союзу для країн Східного партнерства. Участь у Програмі сприяє підвищенню можливостей ДСНС України з подолання катастроф на місцевому, регіональному та національному рівнях шляхом налагодження ефективної взаємодії з ЄС та державами-учасниками Східного партнерства у сфері цивільного захисту [63].

Крім того, участь українських експертів в заходах, передбачених Програмою з попередження, готовності та реагування на катастрофи природного та техногенного характеру для країн Східного партнерства, дозволяє оволодіти спеціальними процедурами ЄС і стандартами з планування, підготовки та проведення рятувальних операцій, підвищити обізнаність з організації цивільного захисту в країнах-учасницях Східного партнерства та сприяти налагодженню взаємодії з відповідними структурами країн-учасниць Східного партнерства у сфері попередження, реагування та ліквідації наслідків надзвичайних ситуацій [63].

Враховуючи вищевикладене, варто погодитись із О. Подскальною, яка зазначає, що реалізації одного із пріоритетів євроінтеграції – приєднання України до Механізму цивільного захисту Європейського Союзу сприятиме підписання та реалізація нової редакції Адміністративної домовленості між ДСНС України та Генеральним Директоратом «Навколишнє середовище» Європейської Комісії щодо співпраці між Координаційним центром реагування на надзвичайні ситуації Механізму цивільного захисту Співтовариства та Оперативно-черговою службою ДСНС України, подальша участь у заходах Програми Європейського Союзу з попередження, готовності та реагування на катастрофи природного та техногенного характеру для країн Східного партнерства (PPRD East) [217, с. 134].

Таким чином, одним із пріоритетних завдань національних органів публічної адміністрації є завершення процесу адаптації національного законодавства у сфері цивільного захисту до права ЄС.

На рівні законів ключовим нормативно-правовим актом у сфері забезпечення безпеки життєдіяльності та цивільного захисту є Кодекс цивільного захисту України, який був введений в дію 1 липня 2013 року та 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 [143].

Правовою основою адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту є також Закон України «Про правовий режим надзвичайного стану» [273].

Вказаний Закон визначає зміст правового режиму надзвичайного стану, порядок його введення та припинення дії, особливості діяльності органів державної влади та органів місцевого самоврядування, підприємств, установ і організацій в умовах надзвичайного стану, додержання прав і свобод людини і громадянина, а також прав і законних інтересів юридичних осіб та відповідальність за порушення вимог або невиконання заходів правового режиму надзвичайного стану [273].

Правовою основою нормотворчості у сфері забезпечення безпеки дорожнього руху є Закон України «Про дорожній рух» [234]. Вказаний Закон регулює суспільні відносини у сфері дорожнього руху та його безпеки,

визначає права, обов’язки і відповідальність суб’єктів – учасників дорожнього руху, міністерств, інших центральних органів виконавчої влади, об'єднань, підприємств, установ і організацій незалежно від форм власності та господарювання [234].

Правовою основою нормотворчості у сфері забезпечення безпеки життєдіяльності є також Закон України «Про охорону праці» [271]. Цей Закон визначає основні положення щодо реалізації конституційного права працівників на охорону їх життя і здоров'я у процесі трудової діяльності, на належні, безпечні і здорові умови праці, регулює за участю відповідних органів державної влади відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища і встановлює єдиний порядок організації охорони праці в Україні [271].

Також правовою основою адміністративно-правового регулювання суспільних відносин у сфері забезпечення безпеки життєдіяльності є Закон України «Про основні принципи та вимоги до безпечності та якості харчових продуктів» [270]. Вказаний Закон регулює відносини між органами виконавчої влади, операторами ринку харчових продуктів та споживачами харчових продуктів і визначає порядок забезпечення безпечності та окремих показників якості харчових продуктів, що виробляються, перебувають в обігу, ввозяться (пересилаються) на митну територію України та/або вивозяться (пересилаються) з неї [270].

Окрему увагу слід приділити особливостям адміністративно-правового регулювання механізму забезпечення безпеки життєдіяльності та цивільного захисту.

Адміністративно-правове регулювання слід розглядати як цілеспрямований владний вплив органів публічної адміністрації за допомогою норм адміністративного права (включаючи акти тлумачення та застосування адміністративно-правових норм) на суспільні відносини, пов’язані із публічним управлінням та адмініструванням, публічними інтересами, з метою

реалізації основних функцій держави, включаючи реалізацію та захист прав і свобод людини.

Ознаками адміністративно-правового регулювання є: використання переважно імперативного методу правового регулювання, що не виключає використання органами публічної адміністрації диспозитивного методу та методу рекомендації; владно-управлінський вплив на суспільні відносини, через який розкриваються основні функції держави як регулятора суспільних відносин; здійснення адміністративно-правового регулювання виключно суб'єктами владних повноважень органів публічної адміністрації; здійснення нормотворчості виключно на підставі, на виконання та у відповідності до законів України.

Адміністративно-правове регулювання суспільних відносин здійснюється на підставі, на виконання та у відповідності до законів, в основному через відомчу нормотворчість у формі наказів центральних органів виконавчої влади, спільних наказів органів публічної адміністрації, проте ключову роль в адміністративно-правовому регулюванні суспільних відносин відіграють постанови Кабінету Міністрів України.

Суспільні відносини, пов'язані із забезпеченням безпеки життєдіяльності та цивільним захистом, безумовно містять публічний інтерес, адже однією з основних функцій держави є забезпечення безпеки населення, захист громадян та навколишнього природного середовища від загроз (небезпек) природного, техногенного, соціального та воєнного характеру.

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 [262].

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 [262].

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 [262].

Також слід відзначити Стратегію національної безпеки України, затверджену Указом Президента України від 14 вересня 2020 року № 392/2020, в якій зазначається, що дедалі більше людей відчувають наслідки зміни клімату та зростання техногенного навантаження на навколишнє природне середовище [306].

Крім того, в Стратегі національної безпеки України зазначено, що наразі: збільшуються кількість та масштаби надзвичайних ситуацій природного і техногенного характеру; виснажується екосфера, зростає споживання невідновлюваних ресурсів; руйнуються екосистеми і біоценози; посилюється негативний вплив біологічних факторів на населення, зростає ймовірність виникнення загроз біологічного походження; високою є загроза виникнення і поширення як уже відомих, так і нових інфекційних хвороб; зростає нерівність, зберігаються інші фундаментальні дисбаланси світового розвитку; не вдається сформувати ефективні інструменти глобального управління; стрімкі технологічні зміни, насамперед в енергетиці та біотехнологіях, розробки у сфері штучного інтелекту тощо докорінно трансформують економіку і суспільство в цілому; стрімко зростає роль інформаційних технологій у всіх сферах суспільного життя; розробляються системи озброєнь на основі нових фізичних принципів, із використанням квантових, інформаційних, космічних, гіперзвукових, біотехнологій, а також технологій у сфері штучного інтелекту, створення нових матеріалів, робототехніки та автономних безпілотних апаратів [306].

Таким чином, в Стратегії національної безпеки України окремо зазначено про нові загрози, які несе з собою розвиток інформаційного суспільства, та підкреслено зростання ролі інформаційних технологій у всіх сферах суспільного життя.

До адміністративно-правових засад побудови та функціонування системи цивільного захисту та забезпечення безпеки життєдіяльності в Україні відноситься цілий ряд постанов Кабінету Міністрів України.

Зокрема, постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1052 затверджене Положення про Державну службу України з надзвичайних ситуацій. Так, у відповідності до вказаного Положення, 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 [221].

Також постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733 затверджено Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту [250].

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 [250].

Крім того, постановою Кабінету Міністрів України від 14 березня 2018 р. № 223 затверджено План реагування на надзвичайні ситуації державного рівня [244]. План реагування на надзвичайні ситуації державного рівня розроблено, зокрема, для впорядкування та координації дій органів державної влади, органів місцевого самоврядування, органів управління та сил цивільного захисту, суб'єктів господарювання, спрямованих на ліквідацію наслідків та надання допомоги постраждалим, у разі загрози виникнення або виникнення надзвичайної ситуації [244].

План реагування на надзвичайні ситуації державного рівня призначений для: оперативного реагування органів управління та сил цивільного захисту, запобігання загибелі людей, зменшення матеріальних втрат та організації першочергового життєзабезпечення постраждалих; організації управління, взаємодії та інформування органів управління та сил цивільного захисту, які залучаються до ліквідації наслідків надзвичайної ситуації; визначення послідовності та обсягів організаційних і практичних заходів із реагування на надзвичайну ситуацію та ліквідацію її наслідків, строків виконання, відповідальних виконавців та необхідних для цього ресурсів [244].

План вводиться в дію у разі загрози виникнення або виникнення надзвичайної ситуації згідно з Порядком класифікації надзвичайних ситуацій за їх рівнями, затвердженим постановою Кабінету Міністрів України від 24 березня 2004 р. № 368 [256] та реалізується шляхом: інформування та оповіщення про загрозу виникнення або виникнення надзвичайної ситуації; переведення органів управління та сил цивільного захисту в режим підвищеної готовності та режим надзвичайної ситуації; дії органів управління та сил цивільного захисту в режимі підвищеної готовності та режимі надзвичайної ситуації; управління під час ліквідації наслідків надзвичайної ситуації; залучення сил цивільного захисту і проведення аварійно-рятувальних та інших невідкладних робіт; взаємодії органів управління та сил цивільного захисту; організації основних видів забезпечення під час проведення аварійно-рятувальних та інших невідкладних робіт і ліквідації наслідків надзвичайної ситуації [244].

Також постановою Кабінету Міністрів України від 9 січня 2014 р. № 11 затверджено Положення про єдину державну систему цивільного захисту [249].

У відповідності до вказаного Положення, єдина державна система цивільного захисту – це сукупність органів управління, сил і засобів центральних та місцевих органів виконавчої влади, Ради міністрів Автономної Республіки Крим, виконавчих органів рад, підприємств, установ та

організацій, які забезпечують реалізацію державної політики у сфері цивільного захисту [249].

Єдина державна система цивільного захисту складається з постійно діючих функціональних і територіальних підсистем. Керівництво єдиною державною системою цивільного захисту здійснює Кабінет Міністрів України, а безпосереднє керівництво діяльністю єдиної державної системи цивільного захисту здійснює Державна служба України з надзвичайних ситуацій [249].

Крім того, згідно із п. 23 Положення про єдину державну систему цивільного захисту, в особливий період єдина державна система цивільного захисту функціонує відповідно до вимог Кодексу цивільного захисту України та з урахуванням особливостей, що визначаються згідно із Законами України «Про правовий режим воєнного стану», «Про мобілізаційну підготовку та мобілізацію», а також іншими нормативно-правовими актами [249].

Постановою Кабінету Міністрів України від 11 лютого 2015 р. № 96 затверджено також Положення про Державну службу України з питань праці [248]. У відповідності до вказаного Положення, Державна служба України з питань праці є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Першого віце-прем'єр-міністра України – Міністра економіки, і який реалізує державну політику у сферах промислової безпеки, охорони праці, гігієни праці, поводження з вибуховими матеріалами промислового призначення, здійснення державного гірничого нагляду, а також з питань нагляду та контролю за додержанням законодавства про працю [248].

Також постановою Кабінету Міністрів України від 5 квітня 1994 р. № 227 затверджено Положення про службу безпеки дорожнього руху міністерств, інших центральних органів державної виконавчої влади, підприємств, їх об'єднань, установ і організацій [253]. Вказаною постановою передбачено, що міністерствам, іншим центральним органам державної виконавчої влади, підприємствам, їх об'єднанням, установам і організаціям незалежно від форм власності та господарювання, що мають транспортні

засоби, які беруть участь у дорожньому русі, необхідно створити службу з безпеки дорожнього руху згідно із зазначеним Положенням, укомплектувавши її кваліфікованими фахівцями, і забезпечити розроблення та проведення заходів щодо запобігання дорожньо-транспортним пригодам [253].

Крім того, постановою Кабінету Міністрів України від 11 лютого 2015 р. № 103 затверджено Положення про Державну службу України з безпеки на транспорті [245]. У відповідності до вказаного Положення Державна служба України з безпеки на транспорті (Укртрансбезпека) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Віце-прем'єр-міністра з відновлення України – Міністра розвитку громад, територій та інфраструктури і який реалізує державну політику з питань безпеки на наземному транспорті [245].

Також постановою Кабінету Міністрів України від 2 вересня 2015 р. № 667 затверджено Положення про Державну службу України з питань безпечності харчових продуктів та захисту споживачів [247]. У відповідності до вказаного Положення, Державна служба України з питань безпечності харчових продуктів та захисту споживачів (Держпродспоживслужба) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України та який реалізує державну політику у сферах безпечності та окремих показників якості харчових продуктів, санітарного законодавства, санітарного та епідемічного благополуччя населення, державного нагляду (контролю) за додержанням заходів біологічної і генетичної безпеки щодо сільськогосподарських рослин під час створення, дослідження та практичного використання генетично модифікованого організму у відкритих системах на підприємствах, в установах та організаціях агропромислового комплексу незалежно від їх підпорядкування і форми власності, здійснення радіаційного контролю за рівнем радіоактивного забруднення сільськогосподарської продукції і продуктів харчування тощо [247].

Крім того, враховуючи тему даного дослідження, слід відзначити постанову Кабінету Міністрів України «Питання Міністерства цифрової трансформації» від 18 вересня 2019 р. № 856, якою затверджено Положення про Міністерство цифрової трансформації України [222], адже саме вказане міністерство здійснює координацію діяльності інших органів публічної адміністрації у сфері цифровізації, тобто впровадження інформаційних технологій.

Суб'єктом нормотворчої діяльності у сфері забезпечення безпеки життєдіяльності та цивільного захисту є Міністерство внутрішніх справ України. Так, у відповідності до п. 4 Положення про Державну службу України з надзвичайних ситуацій, затвердженого постановою Кабінету Міністрів України від 16 грудня 2015 року № 1052, 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 [246].

Таким чином, накази, якими регулюються суспільні відносини у сфері цивільного захисту, видаються Міністром внутрішніх справ. Крім того, ДСНС в межах повноважень, передбачених законом, на основі та на виконання Конституції та законів України, актів Президента України, постанов Верховної Ради України, актів Кабінету Міністрів України, наказів МВС видає накази організаційно-розпорядчого характеру, організовує та контролює їх виконання.

В якості прикладів нормотворчої діяльності Державної служби України з надзвичайних ситуацій та Міністерства внутрішніх справ України слід навести накази МВС України: від 29.05.2014 № 523 «Про затвердження Типового положення про територіальні курси, навчально-методичні центри цивільного захисту та безпеки життєдіяльності»; від 03.07.2014 № 631 «Про затвердження Положення про Оперативно-рятувальну службу цивільного

захисту Державної служби України з надзвичайних ситуацій»; від 04.09.2014 № 905 «Про затвердження Вимог до переліку та змісту документів для надання експертного висновку про рівень надзвичайної ситуації»; від 30.12.2014 № 1417 «Про затвердження Правил пожежної безпеки в Україні»; від 26.12.2014 № 1406 «Про затвердження Положення про штаб з ліквідації наслідків надзвичайної ситуації та Видів оперативно-технічної і звітної документації штабу з ліквідації наслідків надзвичайної ситуації»; від 20.02.2015 № 189 «Про затвердження Положення про організацію службової підготовки осіб рядового і начальницького складу служби цивільного захисту»; від 30.04.2015 № 500 «Про затвердження Інструкції про порядок обміну інформацією у сфері запобігання виникненню та реагування на надзвичайні ситуації між Державною службою України з надзвичайних ситуацій і Адміністрацією Державної прикордонної служби України»; від 15.06.2015 № 696 «Про затвердження Інструкції про порядок утримання, обліку та перевірки технічного стану джерел зовнішнього протипожежного водопостачання»; від 02.11.2015 №1337 «Деякі питання проведення перевірок щодо додержання суб'єктом господарювання вимог законодавства у сфері цивільного захисту, техногенної та пожежної безпеки»; від 04.05.2016 № 356 «Про затвердження Положення про підсистему реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт єдиної державної системи цивільного захисту»; від 22.08.2016 № 859 «Про затвердження Інструкції про порядок взаємодії між Державною службою України з надзвичайних ситуацій, Національною поліцією України та Національною гвардією України у сфері запобігання і реагування на надзвичайні ситуації, пожежі та небезпечні події» [186].

Крім того, в якості прикладу спільної нормотворчої діяльності у сферах забезпечення безпеки життєдіяльності та цивільного захисту слід відзначити спільний наказ МВС України та Держатомрегулювання України від 27.07.2016 № 724/110 «Про затвердження Інструкції про організацію інформаційної взаємодії Державної служби України з надзвичайних ситуацій і Державної

інспекції ядерного регулювання України у сфері запобігання виникненню та реагування на надзвичайні ситуації», спільний наказ МВС України та Державіаслужби України від 25.11.2014 № 1273/602 «Про затвердження Інструкції про порядок обміну інформацією у сфері запобігання надзвичайним ситуаціям та реагування в разі їх виникнення між ДСНС України і Державіаслужбою України», спільний наказ МВС України та Державного агентства автомобільних доріг України від 16.02.2015 № 162/61 «Про затвердження Інструкції про порядок обміну інформацією у сфері запобігання виникненню надзвичайних ситуацій та реагування в разі їх виникнення між Державною службою України з надзвичайних ситуацій і Державним агентством автомобільних доріг України» та спільний наказ МВС України та Мінрегіону України від 12.09.2016 № 920/251 «Про затвердження Інструкції про порядок обміну інформацією у сфері запобігання виникненню та реагування на надзвичайні ситуації між Державною службою України з надзвичайних ситуацій і Міністерством регіонального розвитку, будівництва та житлово-комунального господарства України [186].

Зазначені підзаконні нормативно-правові акти становлять безпосередній зміст адміністративно-правового регулювання у сферах забезпечення безпеки життєдіяльності та цивільного захисту.

Із останніх прикладів нормотворчості у вказаній сфері суспільних відносин слід відзначити наказ МВС України від 20.04.2023 № 326 «Про затвердження Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ» [255].

Так, у відповідності до Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ, СУСЗ – це інтегрована інформаційно-комунікаційна система, що забезпечує збирання, зберігання, використання, передачу, захист інформації про сили та засоби цивільного захисту, об’єкти, на яких існує загроза виникнення надзвичайних ситуацій,

пожеж та інших небезпечних подій, у тому числі об’єкти підвищеної небезпеки, надзвичайні ситуації, небезпечні події, у тому числі пожежі, а також іншої інформації, необхідної для керування силами та засобами цивільного захисту, а також оперативно-диспетчерського управління ними [255].

Володільцем інформації, що обробляється в СУСЗ, є ДСНС, яка забезпечує збереження та захист інформації від випадкової втрати або знищення, незаконної обробки та незаконного доступу до інформації. Власником СУСЗ є держава в особі ДСНС, яка здійснює організаційне та методологічне функціонування СУСЗ, контроль за дотриманням вимог ведення СУСЗ. Адміністратором СУСЗ є визначена власником СУСЗ установа, що належить до сфери управління ДСНС і забезпечує: реалізацію заходів з інформаційного, технічного і програмно-технологічного функціонування СУСЗ; визначення порядку та правил управління інформаційною безпекою, політики та підходів до управління ризиками; відповідно до компетенції надання, обмеження, припинення користувачам доступу до СУСЗ у випадках, передбачених цим Положенням та іншими нормативно-правовими актами, визначеними законодавством; здійснення заходів зі створення, підтримки та технічного адміністрування інформаційно-комунікаційних засобів, програмних та апаратних компонентів, що використовуються для забезпечення функціонування СУСЗ; реалізацію інформаційної взаємодії та інтеграцію з іншими реєстрами, електронними інформаційними ресурсами, засобами центральної підсистеми єдиної інформаційної системи Міністерства внутрішніх справ; організацію впровадження та вдосконалення програмно-апаратних засобів ведення СУСЗ; збереження та захист інформації від втрати, знищення, незаконної обробки та незаконного доступу до інформації, що міститься в ресурсах СУСЗ; організація заходів із створення, упровадження, забезпечення функціонування та адміністрування ресурсів СУСЗ; здійснення заходів із кібербезпеки [255].

Крім того, у відповідності до Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ, суб'єктами СУСЗ є ДСНС, територіальні органи ДСНС, установи, організації і підприємства, що належать до сфери управління ДСНС. Електронна інформаційна взаємодія суб'єктів СУСЗ здійснюється з використанням засобів СУСЗ. Користувачами СУСЗ є фізичні особи та уповноважені посадові особи суб'єктів СУСЗ, яким у встановленому порядку надано відповідні права доступу до ресурсів СУСЗ. Комплексна система захисту інформації забезпечує захист інформації в СУСЗ шляхом здійснення комплексу технічних, криптографічних, організаційних та інших заходів і використання засобів захисту інформації, спрямованих на недопущення блокування доступу до інформації, несанкціонованого доступу та/або її модифікації. Обробка та захист інформації в СУСЗ здійснюються відповідно до вимог Законів України «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних» та інших нормативно-правових актів [255].

Окремо слід зазначити, що згідно із вказаним Положенням, завданням СУСЗ є автоматизація основних службових процесів для управління силами та засобами цивільного захисту, контролю розвитку подій під час ліквідації наслідків надзвичайних ситуацій, небезпечних подій, у тому числі пожеж, а також оперативно-диспетчерського управління ними до рівня стандартів операційних процедур та автоматизованого робочого місця користувача, забезпечення формування, зберігання, спільного використання і верифікації суб'єктами та користувачами СУСЗ інформаційних ресурсів СУСЗ [255].

Функціональні можливості СУСЗ забезпечують: обмін потоками інформації із ЦП ЄІС МВС; обробку інформації, що формується у процесі діяльності суб'єктів та користувачів СУСЗ; перевірку своєчасності внесення, достовірності та повноти інформації, яка відповідно до законодавства обробляється суб'єктами та користувачами СУСЗ, за напрямами їх діяльності; систематизацію та узагальнення інформації, перетворення у формат,

придатний для проведення подальшого аналізу та забезпечення роботи автоматизованих підсистем підтримки прийняття рішень, сигнальних і контрольних сервісів; автоматизацію та верифікацію процесів інформаційної діяльності суб'єктів та користувачів СУСЗ в інтерактивному режимі реального часу; комплексний захист інформації, що міститься в електронних інформаційних ресурсах СУСЗ; автентифікацію та авторизацію суб'єктів та користувачів, інформаційних або інформаційно-комунікаційних систем та/або походження та цілісність електронних даних; логічний контроль та контроль повноти інформації для кожного інформаційного об'єкта; синтаксичний та семантичний контроль, контроль за повнотою файлів інформаційного обміну; ведення та зберігання системних журналів аудиту роботи суб'єктів та користувачів СУСЗ, реєстрації роботи програмних засобів, аудиту засобів безпеки, аудиту приймання-передавання інформації; повідомлення про помилки (проблеми) під час обробки та обміну потоками інформації; збереження електронних інформаційних ресурсів у спеціальному електронному архіві та їх автоматизоване надсилання до інших електронних інформаційних ресурсів, у тому числі для підготовки та автоматизованого формування статистичних даних, узагальнюючих та аналітичних показників, звітності про виконання завдань тощо [255].

У зв'язку з останнім із наведених прикладів нормотворчості слід зазначити, що використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності також пов'язано із публічним інтересом – оптимізувати (автоматизувати), удосконалити механізми забезпечення безпеки життєдіяльності та цивільного захисту.

Адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності забезпечує єдиний, стандартизований підхід до використання відповідного ліцензованого програмного забезпечення для автоматизації систем забезпечення безпеки життєдіяльності, тобто сумісність цифрових продуктів, які використовуються різними органами публічної адміністрації. Крім того, адміністративно-правове

регулювання вказаних суспільних відносин дозволяє забезпечити належний рівень захисту інформаційних ресурсів шляхом їх централізованого криптографічного шифрування, а також дозволяє оперативно поширювати позитивний досвід використання певного програмного забезпечення, окремих технічних засобів на територію всієї держави.

Однією з провідних інформаційних технологій, використання якої може значно удосконалити єдину державну систему цивільного захисту, є технологія штучного інтелекту, яка наразі врегульована лише на рівні Концепції [281].

Отже, існує об'єктивна необхідність адміністративно-правового регулювання використання інноваційних інформаційних технологій у сферах забезпечення безпеки життєдіяльності та цивільного захисту.

Також слід відзначити, що правове регулювання будь-яких суспільних відносин, включаючи суспільні відносини у сфері забезпечення безпеки життєдіяльності, має базуватися на фундаментальних принципах права, що забезпечує правильне розуміння правової матерії, а також правильній вибір методів та способів правового регулювання конкретних суспільних відносин.

Принципи права так чи інакше досліджують всі науковці у сфері юриспруденції, адже принципи права є його фундаментальними, вихідними ідеями і кожне наукове дослідження має спиратись на основоположні правові принципи. Із наукових робіт, які безпосередньо присвячені принципам права слід виділити роботи А. Колодія «Принципи права: генеза, поняття, класифікація та реалізація» [145], С. Погребняка «Основоположні принципи права (змістовна характеристика)» [215], О. Уварової «Принципи права у правозастосуванні: загальнотеоретична характеристика» [316].

Так, на думку А. Колодія, принципи права – це такі відправні ідеї його буття, які виражають найважливіші закономірності, є однопорядковими із сутністю права та утворюють його основні риси, відрізняються універсальністю, вищою імперативністю і загальнозначимістю, відповідають об'єктивній необхідності побудови та зміцнення певного суспільного ладу.

Принципи права спрямовують і надають синхронності всьому механізмові правового регулювання суспільних відносин. Саме принципи права є критерієм законності та правомірності дії громадян і посадових осіб, адміністративного апарату і органів юстиції [145, с. 43].

До загальних принципів права науковці відносять принципи верховенства права, законності, рівності всіх перед законом та судом, справедливості, презумпції невинуватості, невідворотності юридичної відповідальності тощо. Причому принцип верховенства права включає в себе три принципи: верховенства ратифікованих норм міжнародного права над нормами національного права, верховенство норм Конституції над нормами інших нормативно-правових актів, верховенство прав і свобод людини в системі правових цінностей.

Крім того, враховуючи публічно-правовий характер правовідносин, пов’язаних із використанням інформаційних технологій у сфері цивільного захисту та забезпечення безпеки життєдіяльності, окремо слід назвати принципи адміністративного права, на яких повинна ґрунтуватись діяльність органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту. Це зокрема принцип належного урядування, який включає в себе принципи: забезпечення участі в ухваленні рішень і належного реагування; відкритості і прозорості; доброчесності й етичної поведінки; ефективності, компетентності і спроможності; відкритості до змін; сталості та довгострокової орієнтованості; поваги до прав людини; забезпечення соціальної згуртованості і підзвітності.

Також слід згадати принцип субординації, який передбачає чітку ієрархічну підпорядкованість нижчих органів публічної адміністрації вищим.

Особливе значення в адміністративному праві має принцип законності, який передбачає, що органи публічної адміністрації зобов’язані діяти за формулою: «заборонено все, крім того, що прямо дозволено законом», яка відображена в положенні ст. 19 Конституції України: «Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов’язані діяти

лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України».

Спеціальні принципи права, які характерні для певної галузі права, як правило закріплюються на рівні профільного законодавства. Відповідно, принципи правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності містяться в кодексах, законах та підзаконних нормативно-правових актах, які встановлюють правові засади цивільного захисту населення та територій від надзвичайних ситуацій, а також в нормативно-правих актах, які регулюють інформаційні відносини, процеси цифровізації тощо.

Так, у відповідності до розділу І «Загальні положення та основні принципи захисту населення і територій» Концепції захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій, схваленої указом Президента України від 26 березня 1999 р. № 284/99, до принципів захисту населення і територій віднесено:

- принцип безумовного примату безпеки, відповідно до якого концепція прогресу поступається місцем концепції безпеки;

- принцип ненульового (прийнятного) ризику, який полягає в намаганні досягти такого рівня ризику на підприємствах, який можна було б розглядати як прийнятний, причому його параметри мають бути обґрунтовані;

- принцип плати за ризик. Розмір плати залежить від потенційної небезпеки техногенних об’єктів і є пропорційним величині можливого збитку. Ця плата може бути розумним самообмеженням споживання суспільства. Ці кошти спрямовуються на створення системи попередньої безпеки та підвищення оплати на виробництвах, де не повною мірою забезпечується безпека (наприклад, вугільні шахти), а також на певні виплати за ризик, що мають стимулювати проведення заходів, спрямованих на забезпечення безпеки;

- принцип добровільності, згідно з яким ніхто не має права наражати людину на ризик без її згоди;

- принцип невід'ємного права кожного на здорове довкілля. Це право має бути гарантоване і захищене законом. Даний принцип передбачає обов'язки фізичних і юридичних осіб забезпечувати таке право і проводити свою діяльність так, щоб не завдавати шкоди довкіллю;

- принцип правової забезпеченості передбачає, що всі аспекти функціонування системи захисту населення і територій регламентуються відповідними законами та іншими нормативно-правовими актами;

- принцип свободи інформації щодо безпеки людини полягає в урахуванні громадської думки під час вирішення питань щодо будівництва небезпечних підприємств;

- принцип раціональної безпеки передбачає максимально можливе економічно обґрунтоване зниження ймовірності виникнення надзвичайних ситуацій і пом'якшення їх наслідків;

- принцип превентивної безпеки – максимально можливе значення ймовірності виникнення надзвичайних ситуацій;

- принцип необхідної достатності і максимально можливого використання наявних сил і засобів визначає обсяг заходів щодо захисту населення і територій у разі загрози надзвичайних ситуацій [262].

Водночас, згідно з ч. 1 ст. 7 «Основні принципи здійснення цивільного захисту» Кодексу цивільного захисту України, цивільний захист здійснюється за такими основними принципами:

- гарантування та забезпечення державою конституційних прав громадян на захист життя, здоров'я та власності, а також виконання у воєнний час норм міжнародного гуманітарного права;

- комплексного підходу до вирішення завдань цивільного захисту;

- пріоритетності завдань, спрямованих на рятування життя та збереження здоров'я громадян;

- максимально можливого, економічно обґрунтованого зменшення ризику виникнення надзвичайних ситуацій;

- централізації управління, єдиноначальності, підпорядкованості, статутної дисципліни Оперативно-рятувальної служби цивільного захисту, аварійно-рятувальних служб;

- гласності, прозорості, вільного отримання та поширення публічної інформації про стан цивільного захисту, крім обмежень, встановлених законом;

- добровільності – у разі залучення громадян до здійснення заходів цивільного захисту, пов'язаних з ризиком для їхнього життя і здоров'я;

- відповідальності посадових осіб органів державної влади та органів місцевого самоврядування за дотримання вимог законодавства з питань цивільного захисту;

- виправданого ризику та відповідальності керівників сил цивільного захисту за забезпечення безпеки під час проведення аварійно-рятувальних та інших невідкладних робіт [143].

Окремо слід виділити принципи інформаційних відносин, які необхідно враховувати в процесі правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Так, у відповідності до ч. 1 ст. 2 Закону України «Про інформацію», основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя [261].

Крім того, у відповідності до ст. 4 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» державне регулювання та управління у сферах електронної ідентифікації та електронних довірчих послуг здійснюється на засадах: забезпечення принципу верховенства права у процесі електронної ідентифікації та надання електронних довірчих послуг; створення сприятливих та конкурентних умов для розвитку та функціонування

сфер електронної ідентифікації та електронних довірчих послуг; забезпечення захисту прав і законних інтересів користувачів послуг електронної ідентифікації та електронних довірчих послуг; відповідності вимог до електронної ідентифікації та надання електронних довірчих послуг національним, європейським та міжнародним стандартам; забезпечення інтероперабельності та технологічної нейтральності технічних рішень, а також недопущення їх дискримінації; забезпечення захисту персональних даних, що обробляються у процесі електронної ідентифікації та надання електронних довірчих послуг тощо [240].

Таким чином, в процесі правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності необхідно спиратись як на загальноправові, так і спеціальні правові принципи, які містяться в Кодексі цивільного захисту населення України, законах та підзаконних актах, якими врегулювано різні аспекти захисту населення і територій у разі виникнення надзвичайних ситуацій, а також враховувати принципи права, які описані в нормативно-правових актах, якими врегульовано інформаційні відносини, зокрема, відносини у сфері використання інформаційних (цифрових) технологій.

До перелічених вище спеціальних принципів правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід додати принципи оперативності та координації. Так, принцип оперативності передбачає своєчасне нормативне врегулювання використання останніх досягнень у сфері цифровізації для запобігання виникненню надзвичайних ситуацій та ліквідації їх наслідків. Принцип координації означає узгодження змісту нових нормативно-правових актів з питань забезпечення безпеки життєдіяльності із уповноваженими посадовими особами Міністерства цифрової трансформації України та прийняття спільних наказів у разі доцільності або необхідності використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в цілому та захисту населення і територій у разі виникнення надзвичайної ситуації зокрема.

До актуальних напрямів адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід віднести:

- адміністративно-правове врегулювання розробки та функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати, серед іншого, інтерактивну мапу захисних укриттів (з можливістю побудови маршруту слідування для особи з урахуванням геолокації), місць локалізації надзвичайних ситуацій та їх наслідків (за виключенням місць прильотів ворожих ракет та безпілотних літальних апаратів), а також інформаційну базу суб'єктів забезпечення цивільного захисту та безпеки життєдіяльності;

- адміністративно-правову регламентацію розробки, поширення (популяризації), а також порядку адміністрування і використання мобільного застосунку, призначеного для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації;

- адміністративно-правове визначення системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які будуть здійснювати адміністрування єдиної інформаційно-телекомунікаційної системи цивільного захисту, а також здійснювати оперативне обслуговування (керування центром управління) мобільного застосунку, призначеного для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації;

- адміністративно-правове врегулювання питання фінансового та матеріально-технічного забезпечення функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб'єктів, які на

добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків;

- адміністративно-правове врегулювання порядку використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності.

Наведений перелік актуальних напрямів адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності не є вичерпним, адже майже щодня з'являються нові інноваційні інформаційні технології, які потребують правового врегулювання та можуть бути використані у різних сферах суспільних відносин, включаючи забезпечення безпеки життєдіяльності.

Щодо способів адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід зазначити, що, враховуючи публічний характер вказаних правовідносин, для їх врегулювання більшою мірою застосовуються заборони та зобов'язання в рамках імперативного методу правового регулювання (який є характерним для адміністративного права). Суб'єкти владних повноважень органів публічної адміністрації повинні діяти у відповідності до спеціально-дозвільного принципу правового регулювання, згідно з яким суб'єктам владних повноважень дозволено лише те, що прямо передбачено законом.

До прикладу – органи публічної адміністрації зобов'язані використовувати лише ліцензоване програмне забезпечення, зокрема, операційні системи та антивірусні програми встановленого зразка з метою забезпечення сумісності програмного забезпечення, запобігання виникненню конфліктів між окремими програмами, а також надійного захисту інформації.

Проте пріоритетність використання імперативного методу правового регулювання в адміністративному праві не означає, що для адміністративно-правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності не можна використовувати диспозитивний та рекомендаційний методи правового регулювання, і відповідно такі способи правового регулювання як дозволи та рекомендації.

Так, суб'єкти владних повноважень можуть бути наділені дискреційними повноваженнями, тобто правом самим обирати ту або іншу модель поведінки.

До прикладу – використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності наразі є дискреційним повноваженням органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, адже питання використання технології штучного інтелекту ще не врегульовано на рівні закону чи підзаконного нормативно-правового акту, тому спроби використання вказаної інформаційної технології носять скоріше експериментальний характер і остаточне рішення у разі виникнення надзвичайної ситуації чи загрози її виникнення повинна приймати людина, зокрема, уповноважена посадова особа ДСНС чи керівник відповідного органу публічної адміністрації, підприємства, установи чи організації.

Питання забезпечення безпеки життєдіяльності та цивільного захисту набувають особливої актуальності в умовах воєнного стану, адже до загроз природного, техногенного та соціального характеру додаються загрози воєнного характеру. До останніх слід віднести можливість ураження цивільного населення прямими артилерійськими або ракетно-бомбовими ударами (включаючи результати атак ударними безпілотними літальними апаратами), осколками снарядів, бомб та ракет, а також фрагментами об'єктів навколишньої обстановки, які прийняли на себе основний удар (фрагментами цегли, бетону, дерев, скла тощо). Також до воєнних загроз слід віднести мінну небезпеку, адже навіть після припинення бойових дій саме цивільне населення часто потерпає від випадкового контакту з мінами та боєприпасами, які не розірвалися. Особливу загрозу становлять міни замасковані під об'єкти природного світу, побутові речі, іграшки тощо.

До особливо небезпечних загроз воєнного характеру слід віднести використання ворожими силами касетних або запалювальних снарядів (боєприпасів), отруйних речовин, тобто хімічної зброї, а також біологічної та ядерної зброї. Використання перелічених видів зброї має за мету завдати

максимального ураження живій силі противника, проте якщо збройне протистояння відбувається на території населених пунктів, використання вказаних засобів ураження завдає максимальної шкоди саме цивільному населенню, чому зокрема ядерну зброю називають зброєю масового знищення.

Враховуючи вищезазначене, цивільний захист населення в умовах воєнного стану має виходити на вищій рівень готовності, а органи публічної адміністрації зобов'язані залучати всі сили та засоби цивільного захисту для запобігання негативному впливу чинників воєнного характеру та ліквідації наслідків надзвичайної ситуації, спричиненої застосуванням відповідної зброї.

Воєнний стан прямо впливає і на забезпечення безпеки життєдіяльності в цілому. Адже в результаті бойових дій часто залишається зруйнована інфраструктура з пошкодженими комунікаціями, що становить окрему загрозу життю та здоров'ю населення. Наприклад, обірвані в результаті обстрілів лінії електропередачі можуть стати причиною ураження струмом цивільних осіб, які опиняться в радіусі дії відповідних негативних факторів.

Особливий характер загроз, чинників воєнного характеру вимагає й особливого підходу до адміністративно-правового регулювання окремих питань забезпечення цивільного захисту та безпеки життєдіяльності в цілому. Так, окремої правової регламентації потребують Базові правила безпеки під час війни, Правила безпеки на звільнених територіях, Порядок дій під час повітряної тривоги (ракетної небезпеки чи небезпеки артобстрілів).

Вищезазначене обумовлює актуальність, а також теоретичну та практичну значимість дослідження особливостей адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану.

Сучасний стан адміністративно-правового регулювання питань цивільного захисту та забезпечення безпеки життєдіяльності в цілому в умовах воєнного стану є задовільним, адже навіть поведінка громадян під час повітряної тривоги не є обов'язковою. Є тільки рекомендації або формальні

накази покинути приміщення та прямувати до найближчого укриття. Внаслідок такого формального ставлення результатом ворожих обстрілів часто стають цивільні особи, які ігнорують сигнали повітряної тривоги та попередження про небезпеку.

Ключову роль в ліквідації наслідків ворожих обстрілів відіграє Державна служба України з надзвичайних ситуацій, яка здійснює безпосереднє керівництво діяльністю єдиної державної системи цивільного захисту.

Науковці зазначають, після підписання Президентом України 24 лютого 2022 року Указу № 64/2022 «Про введення воєнного стану в Україні» система цивільного захисту України повинна була працювати у нових реаліях. Небезпечні умови роботи рятувальників вимагали нових, особливих підходів до вирішення проблем по забезпеченню цивільного захисту в період воєнного стану. Головне завдання – безпека самих рятувальників при виїзді на виклики, під час гасіння пожеж на об’єктах критичної інфраструктури. В зону воєнних дій потрапили хімічно небезпечні об’єкти та об’єкти, де знаходяться радіоактивні речовини. Крім того, суттєво підвищилась потенційна загроза використання хімічної або ядерної зброї. Звичайно, вся територія бойових дій, а це – сотні тисяч квадратних кілометрів, піддалась забрудненню різноманітними вибухонебезпечними предметами. І основною роботою на звільнених територіях є саме розмінування та видалення вибухонебезпечних предметів. Потужні удари ворога по об’єктах енергетики призвели до масштабних блекаутів по всій території країни, з наслідками від яких постійно доводиться боротися [195, с. 11].

За результатами узагальнення позитивного досвіду організації цивільного захисту була підготовлена колективна монографія «Особливості цивільного захисту в умовах воєнного конфлікту», в якій зібрано унікальний досвід рятувальників України з організації цивільного захисту населення в умовах воєнних дій [195].

Н. Клименко також зазначає, що Єдина державна система цивільного захисту з 24 лютого 2022 року функціонувала одночасно у двох режимах: режимі надзвичайної ситуації, встановленому з метою ліквідації наслідків медико-біологічної надзвичайної ситуації природного характеру державного рівня і забезпечення санітарного й епідемічного благополуччя населення, та перебувала у готовності до виконання завдань за призначенням в особливий період, у тому числі у воєнний час, з урахуванням особливостей, що визначаються згідно з нормами міжнародного гуманітарного права, законами України «Про правовий режим воєнного стану» та «Про мобілізаційну підготовку та мобілізацію». На її територіальні та функціональні підсистеми й сили цивільного захисту покладалася ліквідація наслідків надзвичайних ситуацій, які відбувалися не тільки в повсякденних умовах, в умовах режиму надзвичайної ситуації та карантину, а й під час воєнного стану [136, с. 227].

Таким чином, особливістю адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану є його здійснення у умовах відповідного правового режиму на підставі, на виконання та у відповідності до спеціальних законів України, якими врегульовано питання функціонування органів публічної адміністрації та суспільства в цілому в умовах правового режиму воєнного стану, а також питання мобілізаційної підготовки та мобілізації в Україні, здійснення мобілізаційних заходів.

У відповідності до ч. 4 ст. 8 Кодексу цивільного захисту України, додатковими завданнями єдиної державної системи цивільного захисту у період дії воєнного стану є: оповіщення органів управління та сил цивільного захисту єдиної державної системи цивільного захисту, а також населення про загрозу застосування чи застосування засобів ураження; введення в дію та реалізація планів цивільного захисту на особливий період; приведення органів управління та сил цивільного захисту, пунктів управління, систем зв’язку та оповіщення у готовність до дій в умовах особливого періоду; організація та проведення рятувальних та інших невідкладних робіт, ліквідації наслідків

надзвичайних ситуацій, які виникли внаслідок воєнних (бойових) дій, у тому числі із застосуванням засобів ураження; переведення органів управління і сил цивільного захисту на штати воєнного часу; розгортання спеціальних формувань, призначених для виконання окремих завдань цивільного захисту на територіях та в населених пунктах, віднесених до груп цивільного захисту, та на об'єктах суб'єктів господарювання, віднесених до категорій цивільного захисту; визначення населених пунктів та районів, що потребують проведення гуманітарного розмінування, маркування небезпечних ділянок, проведення очищення (розмінування) територій; уточнення потреби в захисних спорудах для укриття населення та приведення у готовність усіх об'єктів фонду захисних споруд цивільного захисту, забезпечення цілодобового доступу до таких об'єктів; організація будівництва захисних споруд цивільного захисту, споруд подвійного призначення та виготовлення (монтування) первинних (мобільних) і облаштування найпростіших укриттів, а також (у разі потреби) відновлення пошкоджених (зруйнованих) об'єктів фонду захисних споруд цивільного захисту; здійснення заходів із забезпечення захисту джерел водопостачання; здійснення заходів із забезпечення сталої роботи або безаварійної зупинки суб'єктів господарювання, забезпечення живучості об'єктів критичної інфраструктури, призначених для життєзабезпечення населення; здійснення постійного радіаційного та хімічного спостереження; здійснення заходів щодо підвищення рівня протипожежного захисту об'єктів та територій; підготовка до роботи органів з евакуації, уточнення документації щодо організації та проведення евакуації населення та матеріальних і культурних цінностей; здійснення заходів з підготовки інфраструктури безпечних районів до прийому евакуйованого населення та матеріальних і культурних цінностей, організація забезпечення життєдіяльності евакуйованого населення та розміщення матеріальних і культурних цінностей; проведення (у разі потреби) за окремим рішенням Кабінету Міністрів України, відповідних місцевих органів виконавчої влади (військових адміністрацій) евакуації населення та матеріальних і культурних цінностей з районів

можливих бойових дій у безпечні райони; навчання населення способам захисту від наслідків надзвичайних ситуацій, спричинених застосуванням засобів ураження; відновлення та підтримання громадського порядку в населених пунктах та на територіях, що зазнали впливу засобів ураження; виконання інших завдань та заходів, передбачених планами цивільного захисту на особливий період [143].

Крім того, у відповідності до ч. 17 ст. 32 Кодексу цивільного захисту України, у період дії воєнного стану військовими адміністраціями відповідно до вимог ст. 8 Закону України «Про правовий режим воєнного стану» встановлюється порядок використання за призначенням об'єктів фонду захисних споруд цивільного захисту, що визначає особливості використання об'єктів усіх форм власності для укриття населення. Зазначений порядок повинен передбачати вимоги щодо приведення будівель, споруд чи їх окремих частин у готовність до використання за призначенням відповідно до встановлених законодавством вимог щодо утримання та експлуатації об'єктів фонду захисних споруд цивільного захисту, а також забезпечення цілодобового безперешкодного доступу до них населення за відповідними сигналами цивільного захисту.

З урахуванням вимог цього порядку центральні органи виконавчої влади, інші органи державної влади, місцеві державні адміністрації та органи місцевого самоврядування, суб'єкти господарювання та інші юридичні особи встановлюють порядок використання населенням (працівниками) об'єктів фонду захисних споруд цивільного захисту, що належать до сфери їх управління або перебувають у їх власності [143].

Таким чином, особливість адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану полягає, у тому числі, в підготовці та прийнятті суб'єктами владних повноважень підзаконних (відомчих) нормативно-правових актів, якими врегульовуються окремі питання організації та функціонування єдиної державної системи цивільного захисту в умовах воєнного стану: порядок дій у

випадку оголошення повітряної тривоги, порядок використання населенням (працівниками) об’єктів фонду захисних споруд цивільного захисту, прийняття окремого рішення про евакуацію населення та матеріальних і культурних цінностей з районів можливих бойових дій у безпечні райони тощо.

Як правило, такими підзаконними (відомчими) нормативно-правовими актами є накази, тобто розпорядчі документи, які видають керівники підприємств, організацій, установ, які діють одноосібно (у відповідності до принципу єдиноначальності при персональній відповідальності за результати управлінської діяльності) в межах своїх повноважень (на підставі, на виконання та у відповідності до законодавства України) задля вирішення основних і оперативних завдань (досягнення мети публічного управління в конкретній ситуації).

Положення про єдину державну систему цивільного захисту затверджено постановою Кабінету Міністрів України від 9 січня 2014 р. № 11.

У відповідності до п. 23 вказаного Положення, в особливий період єдина державна система цивільного захисту функціонує відповідно до вимог Кодексу цивільного захисту України та з урахуванням особливостей, що визначаються згідно із Законами України «Про правовий режим воєнного стану», «Про мобілізаційну підготовку та мобілізацію», а також іншими нормативно-правовими актами [249].

Переведення єдиної державної системи цивільного захисту у режим функціонування в умовах особливого періоду здійснюється відповідно до актів Президента України, Кабінету Міністрів України, планів цивільного захисту на особливий період.

З моменту оголошення рішення про мобілізацію (крім цільової) або доведення його до виконавців стосовно прихованої мобілізації чи введення воєнного стану в Україні або в окремих її місцевостях єдина державна система цивільного захисту переводиться у режим функціонування в умовах

особливого періоду в повному обсязі або у межах відповідних регіонів (п. 25 Положення про єдину державну систему цивільного захисту) [249].

Причому передбачено, що підготовка єдиної державної системи цивільного захисту до виконання завдань цивільного захисту в умовах особливого періоду здійснюється завчасно у мирний час, а виконання завдань цивільного захисту під час функціонування єдиної державної системи цивільного захисту в умовах особливого періоду здійснюється у взаємодії з відповідним військовим командуванням [249].

Таким чином, ще однією особливістю адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану є взаємодія із відповідним військовим командуванням в процесі прийняття рішень.

Наприклад, в умовах воєнного стану рішення про проведення обов'язкової евакуації в примусовий спосіб дітей з їх батьками (або особами, які їх замінюють, або іншими законними представниками) з окремого населеного пункту в місцевості, де ведуться бойові дії, приймають обласні військові адміністрації за погодженням з органами військового командування на відповідній території та Координаційним штабом з питань проведення обов'язкової евакуації населення.

До правових засад адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану також слід віднести Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, затверджене постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733 [250].

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 [250].

У відповідності до п. 30-1 Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, після отримання інформації про загрозу виникнення або виникнення надзвичайних ситуацій воєнного характеру від чергових змін пунктів управління органів військового управління Збройних Сил України оперативно-чергова служба на пункті управління ДСНС негайно засобами загальнодержавної автоматизованої системи централізованого оповіщення здійснює оповіщення центральних органів виконавчої влади, що створюють функціональні підсистеми єдиної державної системи цивільного захисту, Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських держадміністрацій, територіальних органів ДСНС через відповідні оперативно-чергові (чергові), оперативно-диспетчерські служби [250].

Крім того, згідно п. 31-1 вказаного Положення, після отримання інформації про загрозу виникнення або виникнення надзвичайних ситуацій воєнного характеру засобами загальнодержавної автоматизованої системи централізованого оповіщення або від чергових змін пунктів управління органів військового управління Збройних Сил України оперативно-чергова (чергова) служба, що здійснює оповіщення в разі загрози виникнення або виникнення надзвичайної ситуації на регіональному (місцевому) рівні, негайно засобами територіальної автоматизованої системи централізованого оповіщення (місцевої автоматизованої системи централізованого оповіщення)

здійснює оповіщення місцевих органів виконавчої влади (органів місцевого самоврядування), підприємств, установ, організацій, органів управління та сил цивільного захисту і населення [250].

Важливим є використання інформаційних технологій для 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. До таких технологій слід віднести використання мобільного застосунку «Повітряна тривога».

Проте, як вже було зазначено вище, проблемним питанням залишається відповідальність суб'єктів владних повноважень, юридичних та фізичних осіб за ігнорування, зокрема, сигналів повітряної тривоги та попередження про підвищену небезпеку ракетних обстрілів.

Як правило, поведінка працівників підприємств, установ та організацій в таких випадках регламентована внутрішніми наказами керівників, які мають формально-рекомендаційний характер і тому, як правило, не виконуються.

Як результат, жертвами ракетно-бомбових ударів, а також атак ударних безпілотних літальних апаратів стає все більша кількість цивільного населення.

Враховуючи вищезазначене, вбачається доцільним регламентувати обов'язкові дії керівництва та працівників підприємств, установ та організації незалежно від форми власності при оголошенні повітряної тривоги, а також обов'язкову поведінку фізичних осіб в публічних місцях під час повітряної тривоги на рівні постанови Кабінету Міністрів України, а також доповнити Кодекс України про адміністративні правопорушення окремою статтею, яка буде передбачати адміністративну відповідальність за недотримання порядку поведінки в публічних місцях під час повітряної тривоги.

Правові засади адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану включають також План реагування на надзвичайні ситуації

державного рівня, затверджений постановою Кабінету Міністрів України від 14 березня 2018 р. № 223 [244].

План реагування на надзвичайні ситуації державного рівня розроблено для впорядкування та координації дій органів державної влади, органів місцевого самоврядування, органів управління та сил цивільного захисту, суб'єктів господарювання, спрямованих на ліквідацію наслідків та надання допомоги постраждалим, у разі загрози виникнення або виникнення надзвичайної ситуації [244].

Вказаний План призначений для: оперативного реагування органів управління та сил цивільного захисту, запобігання загибелі людей, зменшення матеріальних втрат та організації першочергового життєзабезпечення постраждалих; організації управління, взаємодії та інформування органів управління та сил цивільного захисту, які залучаються до ліквідації наслідків надзвичайної ситуації; визначення послідовності та обсягів організаційних і практичних заходів із реагування на надзвичайну ситуацію та ліквідацію її наслідків, строків виконання, відповідальних виконавців та необхідних для цього ресурсів. План реалізується шляхом: інформування та оповіщення про загрозу виникнення або виникнення надзвичайної ситуації; переведення органів управління та сил цивільного захисту в режим підвищеної готовності та режим надзвичайної ситуації; дії органів управління та сил цивільного захисту в режимі підвищеної готовності та режимі надзвичайної ситуації; управління під час ліквідації наслідків надзвичайної ситуації; залучення сил цивільного захисту і проведення аварійно-рятувальних та інших невідкладних робіт; взаємодії органів управління та сил цивільного захисту; організації основних видів забезпечення під час проведення аварійно-рятувальних та інших невідкладних робіт і ліквідації наслідків надзвичайної ситуації [244].

Отже, до особливостей адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану слід віднести постійну підвищену готовність єдиної державної системи цивільного захисту (органів управління та сил цивільного захисту) до

ліквідації надзвичайних ситуацій, які викликані чинниками воєнного характеру, зокрема, виникли в результаті ворожих ракетно-бомбових ударів, атак безпілотних літальних апаратів, артилерійських обстрілів тощо.

Особливу роль в ліквідації наслідків надзвичайних ситуацій в умовах воєнного стану відіграють добровольці, тобто фізичні особи, які знаходяться або проживають в безпосередній близькості від місць локалізації наслідків надзвичайних ситуації, зокрема, об'єктів цивільної інфраструктури, які зруйновані в результаті ворожих обстрілів, ракетних або бомбових ударів.

З метою удосконалення порядку залучення добровольців для ліквідації наслідків надзвичайних ситуацій в умовах воєнного стану доцільно розробити та поширити мобільний застосунок з перспективною назвою «Я – доброволець», через який фізичні особи в режимі онлайн зможуть долучитися до національної бази добровольців та у випадку настання надзвичайної ситуації оперативно прибути на місце локалізації її наслідків. Завдяки можливості використання даних геолокації автоматизована система зможе чітко визначити тих добровольців, які знаходяться неподалік місця події та надіслати їм повідомлення про можливість долучитися до ліквідації наслідків надзвичайної ситуації. Крім того, за допомогою вказаного перспективного мобільного застосунку керівництво та спеціалісти Державної служби України з надзвичайних ситуацій зможуть координувати роботу зазначених добровольців, надавати їм рекомендації та поради, вести облік вказаних суб'єктів тощо.

Відповідно, розробка та порядок використання вказаного перспективного мобільного застосунку «Я – доброволець» потребують детального адміністративно-правового врегулювання на рівні спільного наказу МВС України (яке є суб'єктом нормотворчої діяльності у даній сфері суспільних відносин [221]) та Міністерства цифрової трансформації України, яке здійснює координацію діяльності органів публічної адміністрації у сфері цифровізації [222].

Таким чином, інноваційні інформаційні технології та їх належна адміністративно-правова регламентація дозволять значно оптимізувати, удосконалити систему цивільного захисту в умовах воєнного стану.

Враховуючи вищезазначене, доцільно розробити та прийняти постанову Кабінету Міністрів України щодо обов'язкових дій керівництва та працівників підприємств, установ та організації незалежно від форми власності при оголошенні повітряної тривоги, а також щодо обов'язкової поведінки фізичних осіб в публічних місцях під час повітряної тривоги. Крім того, пропонується внести зміни до Кодексу України про адміністративні правопорушення щодо встановлення адміністративної відповідальності за невиконання обов'язкових дій під час повітряної тривоги.

Питання щодо розробки, правової регламентації та впровадження в діяльність ДСНС України перспективного мобільного застосунку «Я – доброволець» буде розглянуто у наступних підрозділах роботи.

2.2 Заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій

Результатом останніх науково-технічних революцій стала цифровізація майже всіх сфер суспільних відносин, впровадження високотехнологічного та роботизованого виробництва, мінімізація ролі людини в технологічних процесах та інші досягнення.

Водночас розвиток та впровадження нових технологій підвищили рівень загрози (ризик) виникнення техногенних аварій та інших надзвичайних ситуацій, а також розширили можливості використання нових технічних засобів та цифрових інструментів із протиправною метою або у військових цілях.

Вищезазначене актуалізує необхідність дослідження заходів забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій техногенного, соціального або природного характеру в контексті

необхідності адміністративно-правового регулювання порядку застосування вказаних заходів та визначення перспективних напрямів удосконалення відповідного національного законодавства в умовах цифровізації суспільних відносин.

Заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій регламентовано на рівні кодексів, законів, постанов уряду, указів Президента України, а також наказів міністерств та інших центральних органів виконавчої влади.

Так, Кодекс цивільного захисту України 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, 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 [143].

Заходи забезпечення безпеки населення і територій при виникненні надзвичайних ситуацій передбачені Розділом IV «Захист населення і територій від надзвичайних ситуацій» Кодексу цивільного захисту України, який включає в себе глави: «Оповіщення та інформування суб'єктів забезпечення цивільного захисту» (глава 6); «Укриття населення в об'єктах фонду захисних споруд цивільного захисту та евакуаційні заходи» (глава 7); «Інженерний захист територій, радіаційний і хімічний захист» (глава 8); «Медичний, біологічний і психологічний захист, забезпечення санітарного та епідемічного благополуччя населення» (глава 9); «Навчання населення діям у надзвичайних ситуаціях» (глава 10) [143].

Кожна із вищезазначених глав містить в собі комплекс відповідних заходів захисту населення і територій від надзвичайних ситуацій, що враховуючи юридичну силу кодексу як нормативно-правового акту дозволяє уніфікувати та систематизувати заходи захисту населення і територій при виникнення надзвичайних ситуацій незалежно від їх виду, а також обрати необхідні заходи для конкретної ситуації.

Показово, що заходи забезпечення безпеки населення і територій при виникненні надзвичайних ситуацій розташовані в Кодексі цивільного захисту України у відповідності до порядку, послідовності застосування. Так, спочатку здійснюється оповіщення та інформування суб'єктів забезпечення цивільного захисту про виникнення надзвичайної ситуації. Саме на цьому етапі ключову роль відіграють сучасні інформаційні технології, а саме, можливості Інтернет, мобільних застосунків тощо. Потім відбувається укриття населення в об'єктах фонду захисних споруд цивільного захисту та евакуаційні заходи, реалізація яких в сучасних умовах також здійснюється з використанням інформаційних технологій, до яких відносяться, наприклад, інтерактивні карти захисних споруд цивільного захисту, розміщені на офіційному сайті ДСНС України. Інші заходи забезпечення безпеки населення і територій при виникненні надзвичайних ситуацій систематизовані в Кодексі цивільного захисту України за предметним принципом, а саме, за основними видами захисту населення та територій. Окремо виділені заходи навчання населення діям у надзвичайних ситуаціях, реалізація яких також наразі здійснюється із використанням інноваційних інформаційних технологій: можливостей соціальних мереж, он-лайн освіти на профільних сайтах, використання мобільних застосунків тощо.

На окрему увагу заслуговує правова регламентація заходів захисту населення і територій в умовах дії правового режиму надзвичайного стану.

Так, у відповідності до ст. 16 «Зміст заходів правового режиму надзвичайного стану» Закону України «Про правовий режим надзвичайного стану» указом Президента України про введення надзвичайного стану в інтересах національної безпеки та громадського порядку з метою запобігання

заворушенням або кримінальним правопорушенням, для охорони здоров'я населення або захисту прав і свобод інших людей на період надзвичайного стану можуть запроваджуватися такі заходи: встановлення особливого режиму в'їзду і виїзду, а також обмеження свободи пересування по території, де вводиться надзвичайний стан; обмеження руху транспортних засобів та їх огляд; посилення охорони громадського порядку та важливих об'єктів національної економіки та об'єктів критичної інфраструктури; заборона проведення масових заходів, крім заходів, заборона на проведення яких встановлюється судом; заборона страйків; примусове відчуження або вилучення майна у юридичних і фізичних осіб [273].

Перелічені заходи покликані обмежити або виключити вплив негативних факторів, які є наслідком техногенних аварій, пожеж, стихійного лиха тощо та впливають на людей, важливі об'єкти національної економіки, об'єкти критичної інфраструктури та навколишнє природнє середовище.

Крім того, ст. 17 Закону України «Про правовий режим надзвичайного стану» передбачено додаткові заходи режиму надзвичайного стану у зв'язку із надзвичайними ситуаціями техногенного або природного характеру. Так, у разі введення надзвичайного стану з підстав, передбачених п. 1 ч. 2 ст. 4 вказаного Закону, крім заходів, передбачених ст. 16 Закону України «Про правовий режим надзвичайного стану», можуть також здійснюватися такі заходи: тимчасова чи безповоротна евакуація людей з місць, небезпечних для проживання, з обов'язковим наданням їм стаціонарних або тимчасових жилих приміщень; встановлення для юридичних осіб квартирної повинності для тимчасового розміщення евакуйованого або тимчасово переселеного населення, аварійно-рятувальних формувань та військових підрозділів, залучених до подолання надзвичайних ситуацій; тимчасова заборона будівництва нових, розширення діючих підприємств та інших об'єктів, діяльність яких не пов'язана з ліквідацією надзвичайної ситуації або забезпеченням життєдіяльності населення та аварійно-рятувальних формувань; встановлення карантину та проведення інших обов'язкових

санітарних та протиепідемічних заходів; запровадження особливого порядку розподілення продуктів харчування і предметів першої необхідності; мобілізація та використання ресурсів підприємств, установ і організацій, незалежно від форми власності, для відвернення небезпеки та ліквідації надзвичайних ситуацій з обов'язковою компенсацією понесених втрат; зміна режиму роботи підприємств, установ, організацій усіх форм власності, переорієнтація їх на виробництво необхідної в умовах надзвичайного стану продукції, інші зміни виробничої діяльності, необхідні для проведення аварійно-рятувальних і відновлювальних робіт; усунення від роботи на період надзвичайного стану, в разі неналежного виконання своїх обов'язків, керівників державних підприємств, установ і організацій, від діяльності яких залежить нормалізація обстановки в районі надзвичайного стану, та покладення тимчасового виконання обов'язків зазначених керівників на інших осіб [273].

Перелічені основні та додаткові заходи часто пов'язані із обмеженням конституційних прав та свобод громадян, що обумовлено необхідністю досягнення публічної мети введення надзвичайного стану – усунення загрози та якнайшвидша ліквідація особливо тяжких надзвичайних ситуацій техногенного або природного характеру, а також усунення негативних наслідків надзвичайної ситуації та збереження життя та здоров'я людей, важливих об'єктів економіки та критичної інфраструктури, захист навколишнього природного середовища.

Також, у відповідності до частин 2-3 ст. 17 Закону України «Про правовий режим надзвичайного стану», з метою ліквідації особливо тяжких надзвичайних ситуацій у мирний час може здійснюватися цільова мобілізація, обсяги і строк проведення якої визначаються в Указі Президента України про введення надзвичайного стану. У виняткових випадках, пов'язаних з необхідністю проведення невідкладних аварійно-рятувальних робіт, допускається тимчасове переведення або залучення на добровільній основі працездатного населення і транспортних засобів громадян для виконання

зазначених робіт за дозволом відповідного керівника аварійно-рятувальних робіт та за умови обов'язкового забезпечення безпеки праці. При цьому забороняється залучення неповнолітніх, а також вагітних жінок до робіт, які можуть негативно вплинути на стан їх здоров'я [273].

Слід відзначити, що цільову мобілізацію з метою ліквідації особливо тяжких надзвичайних ситуацій у мирний час, а також в період дії правового режиму воєнного стану, доцільно здійснювати із використанням сучасних інформаційних технологій, зокрема, можливостей мобільних застосунків. Останні дозволяють оперативно створити базу даних громадян, які можуть та бажають особисто прийняти участь в ліквідації надзвичайної ситуації та її наслідків, визначити місцезнаходження (геолокацію) вказаних осіб та оперативно надіслати сповіщення (повідомлення) всім зареєстрованим в базі даних добровольцям про час та місце виникнення надзвичайної ситуації, необхідні сили та засоби для її ліквідації, а також можливість прийняти особисту участь в пошуково-рятувальних роботах.

Крім того, згідно з ч. 4 ст. 17 Закону України «Про правовий режим надзвичайного стану», з метою невідкладного вивезення населення, яке підлягає евакуації, у разі безпосередньої загрози його життю або здоров'ю допускається використання транспортних засобів громадян із наступною компенсацією їм витрат у порядку, встановленому Кабінетом Міністрів України [273].

Аналогічно до бази даних добровольців, за допомогою інформаційних технологій доцільно створити базу даних транспортних засобів, власники яких готові надати їх добровільно для організації невідкладного вивезення населення, яке підлягає евакуації при виникненні надзвичайної ситуації.

Отже, актуальним напрямом удосконалення механізму цільової мобілізації людських та матеріальних ресурсів є цифровізація цього процесу із використанням мобільного застосунку, зокрема, шляхом створення бази даних добровольців – громадян, які готові в будь-який момент прийняти участь в ліквідації наслідків надзвичайної ситуації, надати свої транспортні

засоби для термінової евакуації населення (із наступною компенсацією їм понесених витрат), а також організації їх термінового оповіщення через мобільний застосунок з урахуванням місця знаходження конкретних добровольців поблизу місця виникнення надзвичайної ситуації або локалізації її наслідків.

Статтею 18 Закону України «Про правовий режим надзвичайного стану» передбачено додаткові заходи правового режиму надзвичайного стану у зв'язку з масовими порушеннями громадського порядку. Так, у разі введення надзвичайного стану з підстав, зазначених у пунктах 2-7 ч. 2 ст. 4 вказаного Закону, додатково можуть здійснюватися такі заходи: запровадження комендантської години (заборона перебувати на вулицях та в інших громадських місцях без спеціально виданих перепусток і посвідчень особи у встановлені години доби); перевірка документів у громадян, а в необхідних випадках – проведення особистого огляду, огляду речей, транспортних засобів, багажу і вантажів, службових приміщень та житла громадян; обмеження або тимчасова заборона продажу зброї, отруйних і сильнодіючих хімічних речовин, а також алкогольних напоїв та речовин, вироблених на спиртовій основі; тимчасове вилучення у громадян зареєстрованої вогнепальної і холодної зброї та боєприпасів, а у підприємств, установ і організацій – також навчальної військової техніки, вибухових, радіоактивних речовин і матеріалів, отруйних і сильнодіючих хімічних речовин; заборона виготовлення і розповсюдження інформаційних матеріалів, що можуть дестабілізувати обстановку; регулювання роботи цивільних теле- та радіоцентрів, заборона роботи аматорських радіопередавальних засобів та радіовипромінювальних пристроїв особистого і колективного користування; особливі правила користування зв'язком та передачі інформації через комп'ютерні мережі; порушення у порядку, визначеному Конституцією і законами України, питання про заборону діяльності політичних партій, громадських організацій в інтересах національної безпеки та громадського

порядку, охорони здоров’я населення або захисту прав і свобод інших людей [273].

Ряд вищезазначених додаткових заходів правового режиму надзвичайного стану також доцільно здійснювати із використанням сучасних інформаційних технологій. Так, реалізацію заборони виготовлення і розповсюдження інформаційних матеріалів, що можуть дестабілізувати обстановку, а також запровадження особливих правил користування зв’язком та передачі інформації через комп’ютерні мережі доцільно здійснювати із застосуванням такої інформаційної технології як штучний інтелект, яка дозволяє використовувати задані алгоритми та інтернет-фільтри для блокування інформації певного змісту, обмеження доступу до комп’ютерних мереж в певних районах або на певний час тощо.

Серед постанов уряду, присвячених правовому регулюванню у сфері забезпечення безпеки життєдіяльності, в якості прикладу можна навести Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв’язку у сфері цивільного захисту, затверджене постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733 [250], яке також містить правові засади реалізації заходів забезпечення безпеки населення і територій при виникненні надзвичайних ситуацій, зокрема заходи спрямовані на оповіщення про загрозу виникнення або виникнення надзвичайних ситуації та організацію зв’язку у сфері цивільного захисту.

Слід зазначити, що сучасні інформаційні технології дозволяють значно оптимізувати процеси організації оповіщення громадян про загрозу виникнення або виникнення надзвичайних ситуацій, зокрема, шляхом використання відповідних мобільних застосунків, можливостей цифрового телебачення та мережі Інтернет в цілому.

Також постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1052 затверджене Положення про Державну службу України з надзвичайних ситуацій. Згідно з вказаною постановою 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 [221].

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 [221].

В напрямах діяльності ДСНС, передбачених більшою частиною інших підпунктів п. 4 Положення про Державну службу України з надзвичайних ситуацій, фактично описані заходи захисту населення та територій, які реалізує ДСНС у разі загрози виникнення або виникнення надзвичайної ситуації. До прикладу, ДСНС України здійснює разом із центральними та місцевими органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами, організаціями прогнозування імовірності виникнення надзвичайних ситуацій, визначає показники ризику та здійснює районування території України щодо ризику виникнення надзвичайних ситуацій. Вказане прогнозування здійснюється за допомогою інноваційних інформаційних технологій, зокрема, комп’ютерних програм, які дозволяють моделювати розвиток поточної ситуації на певному об’єкті чи на певній території, виявити тенденції змін у навколишньому природному середовищі, враховуючи всі фактори, які впливають або можуть вплинути на нього. До прикладу, науковці моделюють землетрус або можливе виверження потенційно небезпечного вулкану, що дозволяє заздалегідь спрогнозувати час

виникнення надзвичайної ситуації та спланувати необхідні заходи цивільно захисту, які необхідно провести у випадку практичної реалізації прогнозу. Для такого моделювання та прогнозування у сфері забезпечення безпеки життєдіяльності та цивільного захисту доцільно використовувати можливості такої інноваційної інформаційної технології як штучний інтелект.

Отже, перспективним напрямом адміністративно-правового врегулювання заходів забезпечення безпеки населення і територій при виникненні надзвичайних ситуацій є правове регулювання використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності.

Так, 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 [150].

В умовах жорсткої світової конкуренції саме розвиток інноваційних технологій повинен стати основним напрямом розвитку національної економіки та ключовим завданням органів публічної адміністрації.

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 [150].

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 [150].

Таким чином, основні питання використання технології штучного інтелекту у всіх сферах суспільних відносин, включаючи забезпечення безпеки життєдіяльності, повинні бути регламентовані на рівні окремого закону.

На увагу заслуговує системне викладення заходів забезпечення безпеки населення і територій в Концепції захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій, схваленої Указом Президента України від 26 березня 1999 р. № 284/99.

Так, згідно із вказаною Концепцією, до основних завдань захисту населення і територій під час 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 [262].

У розділі ІІІ Концепції захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій визначено основні заходи захисту населення і територій від надзвичайних ситуацій. Зокрема передбачено, що з метою захисту населення, зменшення втрат та шкоди економіці в разі виникнення надзвичайних ситуацій має проводитися спеціальний комплекс заходів, який має такі складові:

- оповіщення та інформування (оповіщення про загрозу і постійне інформування населення досягається завчасним створенням і підтримкою в постійній готовності загальнодержавної і територіальних автоматизованих систем централізованого оповіщення населення – автоматизація досягається використанням інформаційних технологій, коли комп'ютерною програмою здійснюється автоматична розсилка повідомлень про виникнення надзвичайної ситуації та її наслідки відповідним адресатам);

- спостереження і контроль (спостереження і контроль за довкіллям, продуктами харчування і водою забезпечується створенням і підтримкою в постійній готовності загальнодержавної і територіальних систем спостереження і контролю з включенням до них існуючих сил та засобів контролю незалежно від підпорядкованості; організацією збору, опрацювання і передачі інформації про стан довкілля, забруднення продуктів харчування, харчової сировини, фуражу, води радіоактивними, хімічними речовинами та інфекційними мікроорганізмами – спостереження і контроль за довкіллям, продуктами харчування і водою доцільно здійснювати із використанням інформаційних технологій – автоматизованих систем, датчиків та відповідного програмного забезпечення, що гарантує неупередженість засобів контролю та об'єктивний контроль стану навколишнього природного середовища, а також харчових продуктів і продовольчої сировини);

- укриття у захисних спорудах (створення фонду захисних споруд досягається шляхом комплексного освоєння підземного простору міст і населених пунктів для взаємопогодженого розміщення в ньому споруд і приміщень соціально-побутового, виробничого і господарського призначення та з урахуванням пристосування і використання частини приміщень для укриття населення в надзвичайних ситуаціях – важливим елементом механізму забезпечення життєдіяльності та єдиної загальнодержавної системи цивільного захисту є інтерактивні карти захисних споруд, укриттів, які дозволяють громадянам за допомогою смартфону та відповідного програмного забезпечення оперативно знаходити найближчі до їх

місцезнаходження укриття (захисні споруди) завдяки засобам визначення геолокації та автоматизованим навігаторам, що дозволяє побудувати індивідуальний маршрут до найближчого укриття);

- евакуаційні заходи (в умовах неповного забезпечення захисними спорудами в містах та інших населених пунктах, які мають об'єкти підвищеної небезпеки, а також у воєнний час основним способом захисту населення є евакуація і розміщення його у позаміській зоні (слід відзначити, що в умовах повномасштабного збройного конфлікту розміщення населення у позаміській зоні вбачається нераціональним і небезпечним, адже застосування ворогом касетних боєприпасів наражає на небезпеку всіх осіб, які знаходяться на відкритій, не захищеній об'єктами нерухомості, місцевості); залежно від обстановки, яка склалася на час надзвичайної ситуації, може бути проведено загальну або часткову евакуацію населення тимчасового або безповоротного характеру; здійснення організованої евакуації, запобігання проявам паніки і недопущення загибелі людей своєчасно забезпечується шляхом: планування евакуації населення; визначення зон, придатних для розміщення евакуйованих з потенційно небезпечних зон; організації оповіщення населення про початок евакуації; організації управління евакуацією; всебічного життєзабезпечення евакуйованого населення у районах позаміської зони; навчанням населення діям під час проведення евакуації – за допомогою сучасних інформаційних технологій, зокрема мобільних застосунків, а також завдяки використанню можливостей соціальних мереж та месенджерів здійснюється координація дій організаторів та учасників евакуації, оперативне оповіщення громадян про напрями та способи евакуації, координати безпечних шляхів та територій на інтерактивних картах тощо);

- інженерний захист (врахування під час розроблення генеральних планів забудови населених пунктів і ведення містобудування особливої схильності регіонів та окремих площ до проявів небезпечних і катастрофічних явищ; забезпечення раціонального розміщення потенційно небезпечних об'єктів з урахуванням можливих наслідків у разі аварій для безпеки

населення і довкілля; будівництво будинків, споруд, інженерних мереж і транспортних комунікацій з заданими рівнями безпеки і надійності; створення комплексних схем захисту населених пунктів та об'єктів господарювання від небезпечних природних процесів; розроблення і здійснення регіональних та місцевих планів запобігання і ліквідації наслідків надзвичайних ситуацій; організація випереджального будівництва протизсувних, протиповеневих, протиерозійних та інших інженерних споруд спеціального призначення; реалізація заходів щодо санітарної охорони території – планування та реалізацію перелічених заходів цивільного захисту також доцільно здійснювати із використанням інформаційних технологій, зокрема, інтерактивних карт населених пунктів, із нанесенням на них вищезазначених потенційно небезпечних об'єктів та зон можливого ураження у випадку техногенних аварій або природних катастроф);

- медичний захист (заходами запобігання або зменшення ступеня ураження людей, своєчасного надання допомоги постраждалим та їх лікування, забезпечення епідемічного благополуччя в районах надзвичайних ситуацій є: планування і використання існуючих сил і засобів органів охорони здоров'я незалежно від їх відомчої належності; своєчасне застосування профілактичних медичних препаратів; контроль за продуктами харчування, питною водою і джерелами водопостачання; завчасне створення і підготовка спеціальних медичних формувань та розгортання необхідної кількості лікувальних закладів; накопичення медичних засобів захисту, медичного та спеціального майна і техніки; контроль за станом довкілля, санітарно-гігієнічною та епідемічною ситуацією; підготовка медичного персоналу та загальне медико-санітарне навчання населення – за допомогою інформаційних технологій доцільно здійснювати автоматизований контроль безпечності продуктів харчування, питної води та джерел водопостачання);

- біологічний захист (захист від біологічних засобів ураження включає своєчасне виявлення чинників біологічного зараження, їх виду і масштабів, проведення комплексу адміністративно-господарських, режимно-

обмежувальних і спеціальних протиепідемічних та медичних заходів; захист від біологічних засобів вимагає: своєчасного використання колективних та індивідуальних засобів захисту; введення режимів карантину та обсервації; знезаражування осередку ураження; проведення екстреної та специфічної профілактики; додержання протиепідемічного режиму об'єктами господарювання, лікувальними закладами і населенням – виявлення чинників біологічного зараження також доцільно здійснювати автоматизованими засобами відбору зразків ґрунту, води тощо, включаючи автоматизовані засоби контролю здоров'я фізичних осіб, зокрема, обладнання, яке дозволяє оперативно зробити аналіз крові, сечі, слини людини тощо);

- радіаційний і хімічний захист (цей захист включає заходи щодо виявлення і оцінки радіаційної та хімічної обстановки, організацію і здійснення дозиметричного і хімічного контролю, розроблення типових режимів радіаційного захисту, забезпечення засобами індивідуального захисту, організацію і проведення спеціальної обробки; виконання вимог даного виду захисту досягається: завчасним накопиченням і підтримкою в готовності засобів індивідуального захисту і приладів радіаційної і хімічної розвідки та контролю; розробленням типових режимів радіаційного захисту населення і функціонування об'єктів господарювання в умовах зараження місцевості; розробленням загальних критеріїв, методів та методик радіаційної та хімічної розвідки і спостережень тощо – радіаційну та хімічну розвідку доцільно здійснювати за допомогою роботизованих систем з використанням технології штучного інтелекту, що дозволить дистанційно вивчати хімічну та радіаційну обстановку на тих об'єктах та територіях, де само перебування людини є небезпечним) [262].

Таким чином, в Концепції захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій достатньо детально та системно описано основні заходи забезпечення безпеки життєдіяльності, що дозволяє формувати концептуальні підходи до ефективної побудови механізму

забезпечення життєдіяльності та цивільного захисту від надзвичайних ситуацій природного, техногенного, соціального або воєнного характеру.

Таким чином, на рівні законів та підзаконних нормативно-правових актів достатньо детально регламентовані заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій та в умовах правового режиму надзвичайного стану.

Проте, варто погодитись із О. Остапенко, який узагальнюючи розгляд адміністративно-правової природи безпеки населення України, зазначає, що незважаючи на достатню нормативно-правову основу адміністративно-правового регулювання відносин у сфері безпеки населення, залишаються проблемними питання практичної реалізації завдань щодо захисту населення від загроз і небезпек природного і техногенного характеру. На стан безпеки впливають негативні фактори соціального, економічного, політичного та ідеологічного змісту, що у сукупності свідчить про потребу здійснення реальної та дієвої політики держави, спрямованої на захист населення України. Водночас О. Остапенко звертає увагу на те, що: безпека людини, суспільства і держави є основою життєдіяльності країни, з урахуванням відносин, що пов’язані з використанням джерел, які є загрозою природного і техногенного змісту; українське суспільство є основною первинною системою забезпечення безпеки людини, що впливає на реалізацію особою своїх потреб і законних інтересів; забезпечення безпеки передбачає створення та функціонування оптимальної і динамічної за напрямами діяльності структури з відповідним нормативно-правовим забезпеченням, що дозволить регулювати відносини у сфері безпеки із запобіганням загрозам та ризикам і створенням належних умов для життєдіяльності людини, суспільства і держави [197, с. 245].

Так, наразі нагальною є потреба правової регламентації використання автоматизованих систем захисту населення і територій (для функціонування яких використовуються інформаційні технології), до яких слід віднести:

- автоматизовані системи оповіщення та інформування населення про надзвичайні ситуації, загрози безпеці життєдіяльності (з використанням мобільних застосунків та Інтернет);

- 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 (з використанням мобільних застосунків та Інтернет);

- 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 не є повним, адже майже щодня з’являються нові цифрові технології, використання яких потребує правового врегулювання, включаючи нові інформаційні технології, які можуть бути використані у сфері забезпечення безпеки життєдіяльності.

Цифровізація заходів забезпечення безпеки життєдільності та цивільного захисту покликана не тільки спростити механізм їх практичної реалізації шляхом автоматизації, але й удосконалити всю систему публічного управління відповідними суспільними відносинами. Проте, не зважаючи на поступову заміну людей в механізмі забезпечення безпеки життєдіяльності роботизованими системами з технологією штучного інтелекту, остаточний контроль за елементами системи цивільного захисту повинен залишатись за

людино, яка здатна прийняти нестандартне та виважене рішення щодо порядку ліквідації надзвичайної ситуації, щодо сил та засобів, які необхідно залучити та застосувати, а також щодо доцільності та порядку евакуації людей, які знаходяться в зоні дії негативних наслідків (чинників) надзвичайної ситуації.

2.3 Національна система суб'єктів забезпечення цивільного захисту та безпеки життєдіяльності

В умовах продовження повномасштабної збройної агресії російської федерації проти України особливої актуальності набувають питання забезпечення безпеки життєдіяльності, адже під ворожі обстріли часто потрапляє цивільна інфраструктура, об'єкти підвищеної небезпеки, що може потягти за собою виникнення надзвичайної ситуації, а також необхідність швидкого реагування сил цивільного захисту, оперативного прибуття рятувальників та інших суб'єктів на місце події.

Значно оптимізувати процеси реагування на виникнення надзвичайної ситуації дозволяють сучасні інформаційні технології, зокрема, засоби мобільного зв'язку, спеціальні мобільні застосунки, бази даних, системи автоматичного реагування на надзвичайні події тощо.

Проте ключову роль в організації оперативного реагування на надзвичайні події та надзвичайні ситуації відіграє людина, а саме, суб'єкти використання вказаних інформаційних технологій, якими є уповноважені посадові особи органу публічної адміністрації, що реалізує державну політику у сфері цивільного захисту, самі рятувальники, а також інші юридичні та фізичні особи, які добровільно надають допомогу або сприяють ліквідації надзвичайної ситуації та її наслідків.

Починаючи дослідження системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в контексті адміністративно-правового регулювання та матеріально-технічного забезпечення ефективного функціонування вказаної системи, слід зазначити,

що забезпечення безпеки життєдіяльності здійснюється за двома основними напрямами. Перший – це забезпечення безпеки життєдіяльності в процесі повсякденної діяльності кожної людини та населення в цілому, яка (діяльність) повинна здійснюватися із урахуванням вимог технічних та техніко-юридичних норм. Другий – це забезпечення безпеки життєдіяльності у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації природного, техногенного, соціального або воєнного характеру.

В залежності від напряму забезпечення безпеки життєдіяльності розрізняються і суб'єкти, які здійснюють відповідну діяльність. Так, безпеку життєдіяльності у повсякденному житті забезпечують як спеціально-уповноважені особи органів публічної адміністрації, такі і самі юридичні та фізичні особи шляхом неухильного дотримання технічних та техніко-юридичних норм.

Так, інспектор з охорони праці та техніки безпеки організовує та координує роботу служби охорони праці підприємства чи організації. Він готує та подає роботодавцю аналізи техніки безпеки і охорони праці, розробляє та надає пропозиції щодо усунення існуючих загроз. Він також надає консультації в галузі охорони праці та техніки безпеки, співпрацює з внутрішніми структурними підрозділами та контролюючими органами, що здійснюють нагляд за умовами праці; дає висновки щодо планів, припущень та проектів модернізації підприємства та бере участь у затвердженні технічних планів нових або відбудованих будівель [122].

Вказаний суб'єкт забезпечення безпеки життєдіяльності також бере участь в оцінці професійного ризику та в розслідуванні нещасних випадків на виробництві, розробляє чи надає висновки щодо внутрішніх інструкцій з техніки безпеки і охорони праці [122].

Крім того, в Україні функціонує такий суб'єкт забезпечення безпеки життєдіяльності як Державна служба з питань праці, яка є центральним органом виконавчої влади, що утворений відповідно до постанови Кабінету Міністрів від 10 вересня 2014 р. № 442 «Про оптимізацію системи центральних

органів виконавчої влади», в результаті реорганізації шляхом злиття Державної служби гірничого нагляду та промислової безпеки та Державної інспекції з питань праці, а також передачі Держсанепідслужбою функцій з реалізації державної політики у сфері гігієни праці та дозиметричного контролю робочих місць і доз опромінення працівників.

Державна служба України з питань праці (Держпраці) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Першого віце-прем'єр-міністра України - Міністра економіки, і який реалізує державну політику у сферах промислової безпеки, охорони праці, гігієни праці, поводження з вибуховими матеріалами промислового призначення, здійснення державного гірничого нагляду, а також з питань нагляду та контролю за додержанням законодавства про працю [248].

До основних завдань Держпраці серед іншого віднесено:

- реалізацію державної політики у сферах промислової безпеки, охорони праці, гігієни праці, поводження з вибуховими матеріалами промислового призначення, здійснення державного гірничого нагляду, а також з питань нагляду та контролю за додержанням законодавства про працю;

- здійснення комплексного управління охороною праці та промисловою безпекою на державному рівні;

- здійснення державного регулювання і контролю щодо охорони праці та промислової безпеки у сфері діяльності, пов'язаної з об'єктами підвищеної небезпеки [248].

Таким чином, Державна служба України з питань праці є ключовим суб'єктом забезпечення безпеки життєдіяльності на виробництвах, в гірничодобувній галузі та в цілому у суспільних відносинах, пов'язаних із працею.

Державне управління у сфері дорожнього руху та його безпеки здійснюється Кабінетом Міністрів України, спеціально уповноваженими на це центральними органами виконавчої влади, органами виконавчої влади в

Автономній Республіці Крим, місцевими органами виконавчої влади, органами місцевого самоврядування (ст. 3 Закону України «Про дорожній рух») [234].

Основним суб'єктом забезпечення безпеки дорожнього руху є Національна поліція. Так, у відповідності до пунктів 11-13 ч. 1 ст. 23 Закону України «Про Національну поліцію», поліція відповідно до покладених на неї завдань: регулює дорожній рух та здійснює контроль за дотриманням Правил дорожнього руху його учасниками та за правомірністю експлуатації транспортних засобів на вулично-дорожній мережі; здійснює супроводження транспортних засобів у випадках, визначених законом; видає відповідно до закону дозволи на рух окремих категорій транспортних засобів; у випадках, визначених законом, видає та погоджує дозвільні документи у сфері безпеки дорожнього руху [264].

Національна поліція має достатньо широкі повноваження, сили та засоби для забезпечення безпеки дорожнього руху та активно використовує інноваційні інформаційні технології для забезпечення безпеки дорожнього руху. Так, на дорогах України активно застосовуються автоматизовані камери відеофіксації порушень Правил дорожнього руху, відповідне програмне забезпечення для регулювання дорожнього руху, а також обробки інформації, отриманої з камер відеоспостереження та ідентифікації транспортних засобів тощо. Перспективними є розробки систем автоматичного обмеження швидкості транспортних засобів у відповідності із швидкісними режимами в населених пунктах, а також використання технології штучного інтелекту для аналізу інформації про стан дорожньої обстановки та вжиття заходів для попередження дорожньо-транспортних пригод шляхом обмеження руху на певних ділянках дороги, обмеження швидкості, перенаправлення транспортних потоків тощо.

Важливу роль в забезпеченні безпеки дорожнього руху відіграють служби безпеки дорожнього руху органів публічної адміністрації України. Так, у відповідності до Положення про службу безпеки дорожнього руху

міністерств, інших центральних органів державної виконавчої влади, підприємств, їх об'єднань, установ і організацій, затвердженого постановою Кабінету Міністрів України від 5 квітня 1994 р. № 227, робота щодо забезпечення безпеки дорожнього руху, запобігання дорожньо-транспортним пригодам у міністерствах, інших центральних органах державної виконавчої влади, на підприємствах, в їх об'єднаннях, установах і організаціях, що мають транспортні засоби, ведеться залежно від чисельності працівників, зайнятих експлуатацією цих засобів, відповідним структурним підрозділом – службою безпеки дорожнього руху або окремими фахівцями з цих питань [253].

Також, у відповідності до Положення про Державну службу України з безпеки на транспорті, центральним органом виконавчої влади, який реалізує державну політику з питань безпеки на наземному транспорті є Державна служба України з безпеки на транспорті (Укртрансбезпека) [245].

До основних завдань Укртрансбезпеки віднесено, у тому числі, реалізацію державної політики з питань безпеки на автомобільному транспорті загального користування, міському електричному, залізничному транспорті; здійснення державного нагляду (контролю) за безпекою на автомобільному, міському електричному, залізничному транспорті [245].

Таким чином, забезпечення безпеки життєдіяльності у сфері дорожнього руху здійснюється системою органів публічної адміністрації, кожен з яких має встановлені чинним законодавством функції та використовує інноваційні інформаційні технології для забезпечення безпеки життєдіяльності у сфері дорожнього руху.

Безпеку життєдіяльності у повсякденному житті населення забезпечує і Державна служба України з питань безпечності харчових продуктів та захисту споживачів (Держпродспоживслужба), яка є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України та який реалізує державну політику у галузі ветеринарної медицини, сферах безпечності та окремих показників якості харчових продуктів, карантину та захисту рослин, ідентифікації та реєстрації тварин, санітарного

законодавства, санітарного та епідемічного благополуччя населення (крім виконання функцій з реалізації державної політики у сфері епідеміологічного нагляду (спостереження) та у сфері гігієни праці та функцій із здійснення дозиметричного контролю робочих місць і доз опромінення працівників), попередження та зменшення вживання тютюнових виробів та їх шкідливого впливу на здоров'я населення, ринкового нагляду в межах сфери своєї відповідальності, державного контролю за додержанням законодавства про захист прав споживачів, за якістю зерна та продуктів його переробки, державного нагляду (контролю) за додержанням заходів біологічної і генетичної безпеки щодо сільськогосподарських рослин під час створення, дослідження та практичного використання генетично модифікованого організму у відкритих системах на підприємствах, в установах та організаціях агропромислового комплексу незалежно від їх підпорядкування і форми власності, здійснення радіаційного контролю за рівнем радіоактивного забруднення сільськогосподарської продукції і продуктів харчування тощо [247].

Державна служба України з питань безпечності харчових продуктів та захисту споживачів (Держпродспоживслужба) також активно використовує інноваційні інформаційні технології у своїй діяльності. Це і відповідні технічні засоби вимірювання рівня вмісту шкідливих речовин в продуктах харчування та в продовольчій сировині, і відповідне програмне забезпечення, яке дозволяє обробляти та систематизувати інформацію, яка стосується діяльності служби, і можливості Інтернет для поширення інформації про появу на ринку України небезпечних харчових продуктів, небезпеку використання певної продовольчої сировини тощо.

Таким чином, питання забезпечення безпеки життєдіяльності у повсякденному житті населення знаходиться в компетенції багатьох суб'єктів владних повноважень перелічених органів публічної адміністрації. Перспективним напрямом наукових досліджень є аналіз сучасного стану та перспектив удосконалення використання інформаційних технологій в

діяльності вищезазначених органів публічної адміністрації, а також адміністративно-правове забезпечення вказаних процесів.

Система суб'єктів забезпечення цивільного захисту передбачена ст. 6 Кодексу цивільного захисту України.

Так, у відповідності до ч. 1 вказаної статті, цивільний захист забезпечується з урахуванням особливостей, визначених Законом України «Про національну безпеку України», суб'єктами, уповноваженими захищати населення, території, навколишнє природне середовище і майно, згідно з вимогами цього Кодексу – у мирний час, а також в особливий період – у межах реалізації заходів держави щодо оборони України.

Суб'єктами забезпечення цивільного захисту є центральні органи виконавчої влади, інші органи державної влади, Рада міністрів Автономної Республіки Крим, місцеві державні адміністрації, органи місцевого самоврядування, суб'єкти господарювання, громадські організації [143].

Згідно з ч. 2 ст. 6 Кодексу цивільного захисту України, координацію діяльності органів виконавчої влади у сфері цивільного захисту у межах своїх повноважень здійснюють: Рада національної безпеки і оборони України та Кабінет Міністрів України.

А у відповідності до ч. 3 вказаної статті, для координації діяльності центральних і місцевих органів виконавчої влади, інших органів державної влади, підприємств, установ та організацій, пов'язаної з техногенно-екологічною безпекою, захистом населення і територій, запобіганням і реагуванням на надзвичайні ситуації:

- Кабінетом Міністрів України утворюється Державна комісія з питань техногенно-екологічної безпеки та надзвичайних ситуацій;

- Радою міністрів Автономної Республіки Крим, обласними, Київською та Севастопольською міськими державними адміністраціями утворюються регіональні комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій;

- районними державними адміністраціями, виконавчими органами міських, районних у містах (у разі їх створення), селищних та сільських рад утворюються місцеві комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій;

- керівними органами підприємств, установ та організацій утворюються комісії з питань надзвичайних ситуацій [143].

Таким чином, і на загальнодержавному, і на місцевому рівні утворюються комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій, тобто колегіальні органи, які здійснюють координацію діяльності органів публічної адміністрації, підприємств, установ та організацій щодо попередження виникнення надзвичайних ситуацій та ліквідації їх наслідків.

Для координації робіт з ліквідації конкретної надзвичайної ситуації та її наслідків на державному, регіональному, місцевому та об'єктовому рівнях можуть утворюватися спеціальні комісії з ліквідації надзвичайної ситуації (ч. 4 ст. 6 Кодексу цивільного захисту України) [143].

Ключовим органом публічної адміністрації, який реалізує державну політику у сфері цивільного захисту є Державна служба України з надзвичайних ситуацій, правової основою діяльності якої є Положення про Державну службу України з надзвичайних ситуацій, затверджене постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1052. Згідно з вказаною постановою 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 [221].

До основних завдань ДСНС віднесено, у тому числі:

- здійснення державного нагляду (контролю) за додержанням і виконанням вимог законодавства у сфері пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб;

- виконання функцій компетентного органу у сфері діяльності, пов'язаної з об'єктами підвищеної небезпеки [221].

Саме ДСНС організовує та забезпечує керівництво Кабінетом Міністрів України єдиною державною системою цивільного захисту; розгортає в разі проведення мобілізації спеціальні формування, призначені для виконання окремих завдань цивільного захисту, на територіях та в населених пунктах, віднесених до груп цивільного захисту, а також на об'єктах суб'єктів господарювання, віднесених до категорій цивільного захисту; координує діяльність своїх сил цивільного захисту під час ліквідації наслідків надзвичайних ситуацій, організовує проведення ними аварійно-рятувальних та інших невідкладних робіт, здійснює контроль за їх проведенням; забезпечує гасіння пожеж, рятування людей, надання допомоги в ліквідації наслідків аварій, катастроф, стихійного лиха та інших видів небезпечних подій, що становлять загрозу життю або здоров'ю людей чи призводять до завдання матеріальних збитків; створює та використовує фінансові ресурси та оперативний матеріальний резерв для запобігання і ліквідації наслідків надзвичайних ситуацій та надання термінової невідкладної допомоги постраждалим тощо [221].

Для ефективного виконання своїх завдань ДСНС також наділена правом здійснювати державний нагляд (контроль) у сфері пожежної та техногенної безпеки щодо виявлення та запобігання порушенням вимог законодавства суб'єктами господарювання (крім суб'єктів господарювання, які займаються незалежною професійною діяльністю за місцем проживання та не використовують найману працю, аварійно-рятувальними службами); перевіряти стан дотримання вимог законодавства у сфері цивільного захисту та складати відповідні акти; здійснювати контроль за виконанням вимог законодавства у сфері цивільного захисту центральними органами виконавчої

влади, місцевими держадміністраціями, іншими органами державної влади та органами місцевого самоврядування шляхом проведення комплексних, контрольних і цільових перевірок; здійснювати контроль за виконанням правил безпеки людей на водних об'єктах; здійснювати контроль за станом готовності об'єктів фонду захисних споруд цивільного захисту до використання за призначенням; організовувати та проводити перевірку стану готовності функціональних і територіальних підсистем єдиної державної системи цивільного захисту та відповідних органів управління ними до дій у разі виникнення надзвичайних ситуацій тощо.

Отже, для виконання покладених на неї завдань Державна служба України з надзвичайних ситуацій має достатньо широкі повноваження та матеріально-технічні ресурси, включаючи засоби цифровізації публічного управління у сфері забезпечення безпеки життєдільності та цивільного захисту.

Крім того, 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 [221].

Таким чином, накази, якими регулюються суспільні відносини у сфері цивільного захисту, видаються Міністром внутрішніх справ. Крім того, ДСНС в межах повноважень, передбачених законом, на основі та на виконання Конституції та законів України, актів Президента України, постанов Верховної Ради України, актів Кабінету Міністрів України, наказів МВС видає накази організаційно-розпорядчого характеру, організовує та контролює їх виконання.

Правове регулювання використання інформаційних технологій у різних сферах суспільних відносин, включаючи сфери цивільного захисту та забезпечення безпеки життєдіяльності, відноситься також до компетенції

такого органу публічної адміністрації як 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 широкосмугового 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 [222].

Крім того, 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 [222].

Таким чином, питання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності доцільніше врегульовувати спільними наказами двох суб’єктів нормотворчої діяльності, а саме, Міністерства внутрішніх справ України та Міністерства цифрової трансформації України.

Співпраця вказаних міністерств у сфері адміністративно-правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту забезпечить урахування в процесі спільної нормотворчості останніх досягнень у сферах цифровізації, інноваційного програмного забезпечення та надійних засобів захисту персональних даних та інформації, що становить державну таємницю.

Так, одним із інноваційних напрямів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності є створення спеціального мобільного застосунку з метою мобілізації людських та матеріальних ресурсів для ліквідації надзвичайних ситуацій та їх наслідків.

Ядром вказаного мобільного застосунку повинна стати база даних осіб, які готові добровільно, за викликом через мобільний застосунок, з’явитися на місце події (місце локалізації надзвичайної ситуації чи її наслідків) та прийняти участь в ліквідації надзвичайної ситуації чи її наслідків (прийняти активну участь в розборі завалів, наданні первинної медичної допомоги постраждалим до приїзду швидкої допомоги, забезпеченні пропускного режиму на певній території тощо).

Адміністрування зазначеного мобільного застосунку доцільно доручити уповноваженим посадовим особам Державної служби України з надзвичайних ситуацій, які утворюватимуть оперативний штаб (центр управління ліквідацією надзвичайної ситуації), модеруватимуть базу даних добровольців та забезпечуватимуть двосторонній інформаційний зв’язок між оперативним штабом та добровольцями, а також здійснюватимуть аналіз оперативної інформації та загальне керівництво процесом ліквідації надзвичайної ситуації та її наслідків.

Висновки до розділу 2

1. Правовою основою адміністративно-правового регулювання у сферах забезпечення безпеки життєдіяльності та цивільного захисту є Конституція України та ратифіковані Верховною Радою України міжнародні нормативно-правові акти, кодекси та закони України. Натомість зміст адміністративно-правового регулювання у вказаній сфері суспільних відносин становлять постанови Кабінету Міністрів України, укази Президента України, накази МВС України та Державної служби України з надзвичайних ситуацій, а також спільні накази органів публічної адміністрації.

Особливістю адміністративно-правого регулювання у сферах забезпечення безпеки життєдіяльності та цивільного захисту є часта спільна нормотворчість органів публічної адміністрації з метою забезпечення обміну інформацією про надзвичайні ситуації та координації діяльності з ліквідації надзвичайних ситуацій та їх наслідків. Ще однією особливістю є часте використання техніко-юридичних (технічних) норм в підзаконних актах.

Окремо слід підкреслити необхідність адміністративно-правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності з метою забезпечення сумісності програмного забезпечення та поширення позитивного досвіду використання інноваційних інформаційних технологій у вказаній сфері суспільних відносин.

2. Заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій достатньо детально регламентовані Кодексом цивільного захисту України. Крім того, заходи захисту населення і територій в умовах дії правового режиму надзвичайного стану регламентовані Законом України «Про правовий режим надзвичайного стану».

Також заходи захисту населення і територій від надзвичайних ситуацій передбачені підзаконними нормативно-правовими актами, серед яких: Концепція захисту населення і територій у разі загрози та виникнення надзвичайних ситуацій, схвалена указом Президента України від 26 березня

1999 р. № 284/99, Положення про Державну службу України з надзвичайних ситуацій, затверджене постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1052, Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, затверджене постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733.

Одним із перспективних напрямів адміністративно-правового врегулювання заходів забезпечення безпеки населення і територій у разі виникнення надзвичайних ситуацій є правове регулювання використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності.

Актуальним напрямом удосконалення механізму цільової мобілізації людських та матеріальних ресурсів у разі виникнення надзвичайної ситуації є цифровізація цього процесу із використанням мобільного застосунку, зокрема, шляхом створення бази даних добровольців – громадян, які готові в будь-який момент прийняти участь в ліквідації наслідків надзвичайної ситуації, включаючи систему їх термінового оповіщення через мобільний застосунок з урахуванням місця знаходження доданих до бази даних добровольців поблизу місця виникнення надзвичайної ситуації або локалізації її наслідків.

Актуальною також є потреба адміністративно-правової регламентації використання автоматизованих систем захисту населення і територій, тобто систем, для функціонування яких використовуються інформаційні (цифрові) технології.

3. Дослідження системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволило сформулювати висновок про те, що, враховуючи зростаючі загрози природнього, техногенного, соціального та воєнного характеру, існує реальна потреба створення єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати інтерактивну мапу та інформаційну базу суб'єктів забезпечення цивільного захисту

Також існує об’єктивна потреба нормативного визначення системи суб’єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які будуть здійснювати адміністрування вказаної інформаційно-телекомунікаційної системи, відповідної бази даних, а також здійснювати оперативне обслуговування (керування центром управління, штабом) мобільних застосунків, призначених для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації.

Враховуючи вищевикладене, існує необхідність внесення змін до чинного національного законодавства щодо адміністративно-правової регламентації створення єдиної інформаційно-телекомунікаційної системи цивільного захисту, а також адміністративно-правової регламентації використання мобільних застосунків у сфері забезпечення безпеки життєдіяльності, включаючи права та обов’язки суб’єктів, які будуть здійснювати адміністрування вказаних мобільних застосунків, а також суб’єктів, які будуть залучатися до ліквідації надзвичайних ситуацій та їх наслідків в якості добровольців з використанням встановленого мобільного застосунку.

Правового врегулювання потребує і питання фінансового та матеріально-технічного забезпечення функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб’єктів, які на добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків.

Зазначені питання доцільно врегулювати на рівні спільного наказу Міністерства внутрішніх справ України та Міністерства цифрової трансформації України, що забезпечить використання останніх інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

РОЗДІЛ 3
ЗАРУБІЖНИЙ ДОСВІД АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ В КОНТЕКСТІ ЦИФРОВІЗАЦІЇ ПУБЛІЧНОГО УПРАВЛІННЯ

3.1 Адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в країнах-членах Європейського Союзу: позитивний досвід для України

Україна прагне набути повноправного членства в Європейському Союзі, тому пріоритетним завданням національних органів публічної адміністрації є адаптація національного законодавства до права ЄС. Однією із основних сфер суспільних відносин, яка потребує належного адміністративно-правового регулювання у відповідності до європейських стандартів, є безпека життєдіяльності. Співробітництво у сфері цивільного захисту передбачено зокрема Угодою про асоціацію між Україною та Європейським Союзом.

Враховуючи вищезазначене, дослідження досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі має як теоретичне, так і практичне значення в рамках даного дослідження.

Починаючи дослідження європейського досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід зазначити, що цифровізація публічного управління взагалі є одним із пріоритетних напрямів політики ЄС.

І. Белова, О. Ярощук та А. Гомотюк зазначають, що одним із важливих факторів високого рівня цифровізації сектору публічних послуг, суспільних та економічних процесів Європейського Союзу є інституціональний аспект, адже на рівні спільноти у 2015 році було затверджено Стратегію Єдиного цифрового ринку (A Digital Single Market Strategy for Europe), основними

цілями якої стали: усунення регуляторних бар'єрів шляхом гармонізації правил та норм ЄС у різних секторах, включаючи електронну комерцію, авторське право, захист даних і телекомунікацій з метою полегшення транскордонної діяльності бізнесу; сприяння транскордонній електронній комерції шляхом створення рівних умов для електронної комерції в ЄС, дозволяючи споживачам і підприємствам купувати та продавати товари та послуги онлайн легше та з більшою впевненістю; підвищення інновацій шляхом підтримки стартапів, малих і середніх підприємств, полегшення доступу до фінансування та сприяння розвитку нових цифрових технологій і послуг; підвищення кібербезпеки. Функціонування єдиного цифрового ринку має на меті посилити кібербезпеку та захист даних у всьому ЄС, гарантуючи, що всі громадяни та підприємства ЄС можуть скористатися можливостями, які надають цифрові технології, одночасно захищаючи свою конфіденційність і безпеку [24, с. 182; 351].

Отже, однією з основних цілей функціонування єдиного цифрового ринку ЄС є посилення кібербезпеки та захист даних на території всього Європейського Союзу, що фактично є частиною системи забезпечення безпеки життєдіяльності громадян держав-членів ЄС.

Одним із аспектів Стратегії єдиного цифрового ринку став План дій електронного уряду на 2016-2020 роки (EU e-government action plan 2016-2020), в якому викладено бачення ЄС єдиного цифрового ринку та окреслено конкретні дії, які необхідно вжити для покращення послуг електронного урядування в ЄС. Він зосереджений на покращенні доступності, орієнтованості на користувача та сумісності державних послуг [354].

Окрім цього, у жовтні 2017 року в ЄС було прийнято Таллінську декларацію про електронний уряд, де було викладено бачення розвитку цифрових публічних послуг у ЄС та окреслено ключові принципи і пріоритети для досягнення цього бачення, серед яких одне з ключових місць посідає забезпечення безпеки та конфіденційності цифрових державних послуг і зміцнення довіри громадян за допомогою відкритих стандартів і сумісних

систем. Також в декларації зазначено, що уряди повинні сприяти інноваціям та експериментам у розробці цифрових державних послуг, використовуючи новітні технології, такі як штучний інтелект і блокчейн, для підвищення ефективності та результативності [24, с. 182-183; 366].

Таким чином, Таллінська декларація стала основою для формування національних законодавств держав-членів ЄС у сфері цифровізації публічних послуг та електронного урядування.

І. Белова, О. Ярощук та А. Гомотюк також зазначають, що окрім Таллінської декларації про електронний уряд, важливими документами щодо регулювання розвитку цифровізації в Європейському Союзі є: Європейська структура сумісності (EIF), яка надає загальний набір стандартів і вказівок для забезпечення легкого доступу до державних послуг і спільного використання в усьому ЄС; Регламент eIDAS, що визначає правила електронної ідентифікації та довірчих послуг у всьому ЄС; Загальний регламент захисту даних (GDPR), який встановлює правила обробки персональних даних у ЄС. Таким чином, Європейський Союз за короткий проміжок часу сформував нормативно-правове поле процесів цифровізації публічних послуг [24, с. 182-183].

Слід відзначити, що сутністю Європейського Союзу є чотири свободи: свобода переміщення фізичних та юридичних осіб, свобода руху капіталів, свобода надання послуг на території всіх держав-членів ЄС та свобода руху товарів. Процеси цифровізації покликані забезпечити дієве удосконалення механізмів реалізації вказаних свобод за допомогою використання інформаційних технологій за єдиними стандартами, що забезпечує сумісність програмного забезпечення контрагентів з різних держав, а також надійний захист інформації.

У березні 2021 року Європейська Комісія запропонувала шлях до Цифрового десятиліття. Ця політична програма керується «Цифровим компасом до 2030 року» – планом досягнення цифрової трансформації економіки та суспільства ЄС. Зазначений цифровий компас спрямований на

безпечну цифрову екосистему, орієнтовану на людину, де громадяни отримують повноваження, а компанії процвітають завдяки цифровому потенціалу. Компас вказує чотири кардинальні точки для цієї траєкторії: цифрові навички, безпечна та ефективна цифрова інфраструктура, цифрова трансформація бізнесу та цифровізація державних послуг [328].

Отже, одним із пріоритетів цифрової стратегії ЄС є забезпечення безпечної цифрової інфраструктури, тобто фактично забезпечення безпеки життєдіяльності громадян ЄС в цифровому просторі та у суспільних відносинах, пов'язаних із використанням цифрових інструментів. Одним із ключових здобутків цифровізації є подолання паперової бюрократії та корупції, адже використання цифрових форматів розрахунків, звітності за використання фінансових ресурсів дозволяє відстежувати всі фінансові потоки, доходи і розходи фізичних та юридичних осіб, сплату податків та інших обов'язкових платежів. Таким чином, забезпечується фінансова безпека та благополуччя кожного громадянина та держави в цілому.

Вказаний політичний порядок денний узгоджується з нормами та стандартами ЄС для посилення цифрового суверенітету ЄС. Низка бюджетних інструментів підтримує інвестиції, необхідні для побудови Цифрового десятиліття Європи на міцній основі. Оскільки цифрові технології є пріоритетом ЄС, вони також є пріоритетними для країн-стратегічних партнерів ЄС щодо створення кращого та більш гармонізованого цифрового середовища. Цілі політики Східного партнерства на період після 2020 року включають цільові дії, які сприятимуть розвитку Єдиного цифрового ринку: інвестиції в конкурентоспроможні та інноваційні економіки, у людей і розвиток знань, у безпеку та кіберстійкість, а також у цифрову трансформацію [328].

Таким чином, для національних органів публічної адміністрації в контексті євроінтеграційних процесів важливо приймати активну участь у розвитку Єдиного цифрового ринку ЄС, залучати інвестиції для розвитку

національного цифрового ринку, включаючи заходи із забезпечення кібербезпеки.

Так, Міністерство цифрової трансформації України відповідно до покладених на нього завдань:

- організовує та координує діяльність органів виконавчої влади, пов'язану з інтеграцією України до Єдиного цифрового ринку ЄС (EU Digital Single Market), а також участю України у програмах ЄС щодо цифрового співробітництва, зокрема у Програмі ЄС «Цифрова Європа» (Digital Europe Programme);

- розробляє акти з метою забезпечення виконання завдань, пов'язаних з участю України у Програмі ЄС «Цифрова Європа» (Digital Europe Programme), зокрема щодо процедури визначення кандидатур для включення у мережу Європейських цифрових інноваційних хабів (European Digital Innovation Hubs) [222].

Крім того, у відповідності до п. 7 Положення ро Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856, Мінцифри у процесі виконання покладених на нього завдань взаємодіє в установленому порядку з іншими державними органами, допоміжними органами і службами, утвореними Президентом України, тимчасовими консультативними, дорадчими та іншими допоміжними органами, утвореними Кабінетом Міністрів України, органами місцевого самоврядування, об'єднаннями громадян, громадськими спілками, профспілками та організаціями роботодавців, відповідними органами іноземних держав і міжнародних організацій, а також з підприємствами, установами та організаціями [222].

Отже, в процесі адміністративно-правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, включаючи питання адаптації національного інформаційного законодавства до права ЄС, відповідному органу публічної адміністрації, який реалізує державну політику у сфері цивільного захисту, доцільно взаємодіяти із

Міністерством цифрової трансформації України та здійснювати правове врегулювання вказаних питань за допомогою спільних наказів.

Окрему увагу в контексті правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі слід приділити GDPR – Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних; про відміну Директиви 95/46/ЄС (GDPR набрав чинності 25 травня 2018 року) [359].

Слід відзначити, що захист персональних даних прямо пов'язаний із забезпеченням безпеки життєдіяльності особи, адже в сучасному інформаційному суспільстві протиправне використання персональних даних певної особи може завдати суттєвої шкоди правам і свободам людини, її власності (наприклад, через доступ до банківських рахунків особи, реєстрів власності тощо).

Основні вимоги GDPR: дотримуватися принципів обробки персональних даних; персональні дані слід обробляти прозоро, справедливо та законно (Lawfulness, fairness and transparency); персональні дані можна обробляти лише для явно вказаних законних цілей (Purpose limitation); збирати та зберігати слід лише мінімальну кількість персональних даних, достатніх для зазначеної мети (Data minimisation); персональні дані мають обмежений термін зберігання, не більше ніж це необхідно для певної мети (Storage limitation); забезпечення точності персональних даних, а також можливості їх редагування та видалення (Accuracy); забезпечення безпеки, цілісності та конфіденційності персональних даних (Integrity and confidentiality); контролер повинен бути готовим і здатним продемонструвати дотримання вищезазначених принципів (Accountability); реалізовувати права суб'єктів даних (право бути поінформованим, право на доступ, право на виправлення даних, право на видалення, право на обмеження обробки, право на мобільність даних, право на заперечення, право не бути об'єктом автоматизованого

рішення, у тому числі профайлінгу, право на ознайомлення з Політикою приватності (Privacy Policy) та Політикою використання файлів cookie (Cookie Policy) [359].

Таким чином, GDPR містить широкий перелік вимог щодо захисту персональних даних особи, виконання яких є умовою забезпечення безпеки особи в інформаційному просторі (цифровому середовищі).

Крім того, кожен суб'єкт даних має право на подання скарги до контролюючого органу, без обмеження будь-якого іншого адміністративного чи судового засобу правового захисту. Суб'єкт даних має право безпосередньо звернутися до суду для захисту своїх прав та інтересів. Відповідно до ст. 82 GDPR будь-яка особа, яка зазнала матеріальної чи моральної шкоди внаслідок порушення Регламенту, має право на отримання відшкодування від контролера або процесора за заподіяну шкоду [359].

Отже, GDPR передбачає механізм судового захисту особи, яка зазнала шкоди внаслідок порушення законодавства про захист персональних даних, що є важливою складовою компенсаційного механізму та способом поновлення порушених прав.

На окрему увагу заслуговують штрафні санкції, передбачені GDPR за порушення вимог щодо захисту персональних даних.

Так, за порушення вимог GDPR передбачені наступні адміністративні штрафи: до 10 млн. євро або 2% від світового річного обороту (залежно що більше) за незначні порушення; до 20 млн. євро або 4% від світового річного обороту (залежно що більше) за серйозні порушення, до яких належать порушення контролером та процесором [359].

Таким чином, GDPR – Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних є ключовим нормативним документом Європейського Союзу, який спрямований на захист персональних даних, причому його юридична дія поширюється і на українські компанії, які здійснюють обробку даних громадян держав-членів ЄС.

Безумовно, в умовах збільшення кількості випадків протиправного використання персональних даних, що становить пряму загрозу безпеці життєдіяльності кожної людини, дані якої протиправно розголошуються або використовуються, вищевказаний загальноєвропейський Регламент має пріоритетне значення для національних органів публічної адміністрації, які здійснюють адаптацію національного законодавства до права ЄС.

Не менш важливе значення для забезпечення безпеки життєдіяльності населення ЄС має Новий Регламент (ЄС) 2024/1689 від 13 червня 2024 року щодо штучного інтелекту [187].

Офіційний журнал Європейського Союзу опублікував Регламент (UE) Європейського Парламенту та Ради № 2024/1689 від 13 червня 2024 року, який встановлює гармонізовані правила щодо штучного інтелекту (англ. Artificial Intelligence Act, AI Act). Цей Закон є першим основним законодавчим актом у світі щодо штучного інтелекту. Проте вказаний Закон передбачає не лише контрольні та регуляторні механізми, він також встановлює рекламні заходи (такі як регуляторні «пісочниці» та заходи для підтримки розвитку систем штучного інтелекту), спрямовані на заохочення розвитку технології щодо штучного інтелекту в соціальному плані [187].

Прийняття вказаного Закону (AI Act) безумовно є революційним, адже питання використання технології штучного інтелекту вже давно потребують належного правового регулювання, враховуючи ті потенційні загрози для безпеки життєдіяльності особи, які несе з собою зазначена інноваційна інформаційна технологія.

Європейський закон про штучний інтелект зобов’язує держави-члени призначити один або декілька компетентних органів для нагляду за дотриманням зобов’язань, які він накладає. На європейському рівні Європейський офіс AI, створений Рішенням Комісії від 24 січня 2024 року, буде наглядовим органом і матиме важливі функції, зокрема щодо нагляду за загальними моделями штучного інтелекту. Повноваження, які влада матиме для забезпечення ефективності Закону про AI, включають повноваження

накладати штрафи. Штрафи за порушення Закону про штучний інтелект встановлюються у відсотках від річного обороту компанії-порушника за попередній фінансовий рік або заздалегідь визначеної суми, якщо вона вища та може зрости до 35 мільйонів євро або 7% від прибутку порушника зафіксованого в загальному світовому річному обороті за попередній фінансовий рік, якщо ця сума вища [187].

Отже, сам розмір штрафних санкцій демонструє розуміння суб'єктами владних повноважень інституцій ЄС важливості та необхідності дотримання закону про штучний інтелект, його особливої ролі в механізмі забезпечення безпеки життєдіяльності в інформаційному просторі (цифровому світі).

Даний Закон надає розробникам і користувачам систем чіткі вимоги та зобов'язання щодо конкретного використання штучного інтелекту, одночасно зменшуючи адміністративний і фінансовий тягар для бізнесу. Зобов'язання, передбачені вказаним Законом можуть стосуватися як постачальників (наприклад, розробника інструменту для перевірки резюме), так і користувачів систем штучного інтелекту (наприклад, банку, який купує цей інструмент перевірки) [184].

Таким чином, слід підкреслити універсальність європейського Закону про штучний інтелект, який містить вимоги як для компаній розробників алгоритмів штучного інтелекту, так і для користувачів технології штучного інтелекту, які потенційно можуть порушити права і свободи людини в процесі використання вказаної інформаційної технології.

Закон про штучний інтелект запроваджує єдину структуру для всіх країн ЄС, засновану на далекоглядному визначенні штучного інтелекту та підході, заснованому на оцінці ризиків [184].

Наприклад, системи штучного інтелекту, які дозволяють урядам або компаніям «оцінювати соціальні показники», вважаються явною загрозою основним правам і свободам людини і тому заборонені. До таких особливо шкідливих випадків застосування технології штучного інтелекту віднесено: експлуатацію вразливостей осіб, маніпулювання та використання підсвідомих

прийомів; соціальний скоринг для державних і приватних цілей; індивідуальну предиктивну поліцію, що ґрунтується виключно на профілюванні людей; нецілеспрямований скрейпінг Інтернету або камер відеоспостереження для отримання зображень обличчя людей для створення або розширення баз даних; розпізнавання емоцій на робочому місці та в навчальних закладах, за винятком, коли це необхідно з медичних причин або з міркувань безпеки (наприклад, моніторинг рівня втоми пілота в процесі виконання ним своїх обов'язків); дистанційну біометричну ідентифікацію в режимі реального часу в загальнодоступних місцях правоохоронними органами (за вузькими винятками, коли це необхідно для попередження або розкриття злочину, пошуку без вісті зниклої особи тощо) [184].

Таким чином, зазначений закон встановлює чіткі обмеження у сфері використання технології штучного інтелекту, коли існує потенційна або наявна загроза порушення основних прав і свобод людини (зокрема, права на свободу та особисту недоторканість, захист персональних даних тощо).

Класифікація ризиків, згідно із вказаним Законом, ґрунтується на цільовому призначенні системи штучного інтелекту, відповідно до чинного законодавства ЄС про безпеку продукції. Класифікація, зокрема, залежить від функції, яку виконує система штучного інтелекту, а також від конкретної мети та способів, для яких використовується система [184].

Так, у відповідності до положень європейського Закону про штучний інтелект, системи штучного інтелекту можна віднести до категорії високого ризику у двох випадках: якщо система штучного інтелекту вбудована як компонент безпеки в продукти, на які поширюється чинне законодавство ЄС про безпеку продукції, або система ШІ є самою такою продукцією (це може бути, наприклад, медичне програмне забезпечення на основі технології штучного інтелекту); якщо система штучного інтелекту призначена для використання в умовах високого ризику відповідно до Закону про штучний інтелект (тобто є пряма вказівка в Законі). Важливо, що норми зазначеного Закону включають приклади використання технології штучного інтелекту в

таких сферах, як освіта, міграція, працевлаштування, діяльність правоохоронних органів [184].

Таким чином, європейський закон про штучний інтелект (Artificial Intelligence Act, AI Act) є базовим правовим інструментом забезпечення безпеки життєдіяльності населення держав Європейського Союзу у суспільних відносинах, пов'язаних із використанням штучного інтелекту.

Складовою системи забезпечення безпеки життєдіяльності в Європейському Союзі є також забезпечення безпеки діяльності користувачів в інтернет-середовищі.

Так, О. Федотова зазначає, що у 2014 році Рада Європи затвердила спеціальну декларацію – Керівні принципи з прав людини для користувачів Інтернету у вигляді спеціальної Рекомендації Комітету Міністрів країнам-учасникам, згідно з якими їм належало: активно вживати заходів для захисту прав і свобод користувачів Інтернету, забезпечуючи повний доступ до послуг та ресурсів; регулярно оцінювати та усувати обмеження прав і свобод в Інтернеті, беручи до уваги той момент, що обмеження, передбачені законом, необхідні у демократичному суспільстві; забезпечувати доступ користувачів до ефективних правових механізмів у разі порушення їхніх прав, співпрацюючи з відповідними установами та структурами; сприяти налагодженню координації відповідних структур як всередині Ради Європи, так і поза нею, з метою впливу на стандарти та процедури захисту прав людини в Інтернеті; залучати приватний сектор до діалогу з державними органами та громадянським суспільством, сприяючи відповідальності підприємств перед суспільством та забезпечуючи прозорість їхньої діяльності [320, с. 85-86; 123].

Також О. Федотова формулює висновок про те, що інформаційна політика ЄС формується з орієнтацію на захист діяльності користувачів в мережі Інтернет, про що безпосередньо свідчать загальноєвропейські правові документи. Задля забезпечення відповідності чинним європейським стандартам в інформаційній галузі, Україні потрібно виробити та застосувати

на практиці ефективні інструменти, що зможуть в найкращий спосіб сприяти реалізації прав та свобод користувачів Інтернету [320, с. 86].

Окрему увагу необхідно також звернути на адаптацію національного законодавства, яке регулює суспільні відносини у сфері цивільного захисту, до відповідних положень права Європейського Союзу.

Так, О. Подскальна зазначає, що механізм цивільного захисту Європейського Союзу – найбільша в світі система надання міжнародної координованої оперативної допомоги при надзвичайних ситуаціях, яка включає різноманітні ресурси і форми допомоги. Рішення про заснування Механізму цивільного захисту Рада Європейського Союзу прийняла 23 жовтня 2001 року в м. Люксембурзі. З урахуванням набутого досвіду 17 грудня 2013 року Європейський парламент та Рада прийняли в м. Брюсселі Рішення № 1313/2013/EU «Про Механізм цивільного захисту Союзу» [217, с. 131].

Основна роль Механізму цивільного захисту полягає у сприянні співпраці у заходах з надання допомоги щодо захисту цивільного населення у разі настання надзвичайних ситуацій, які можуть вимагати прийняття термінових заходів реагування. Це відноситься і до ситуації, де може бути безпосередня загроза таких великих надзвичайних ситуацій. Механізм складається із ряду елементів і дій, що включають, у тому числі, і встановлення та управління центром моніторингу і інформації; встановлення і управління загальною аварійною системою зв’язку та інформації. Основною складовою, операційним ядром Механізму цивільного захисту є Координаційний центр реагування на надзвичайні ситуації, що діє під егідою Європейської комісії в м. Брюсселі, працює цілодобово без вихідних та надає країнам доступ до платформи цивільного захисту Європейського Співтовариства [217, с. 131].

Таким чином, в Механізмі цивільного захисту Європейського Союзу активно використовуються інформаційні технології, зокрема, інформаційні платформи, бази даних, засоби оперативного зв’язку. Відповідно, використання вказаних інформаційних технологій має належну правову

регламентацію на рівні рішень Європейського парламенту та Європейської Ради.

Крім того, О. Подскальна справедливо зазначає, що розбудова сучасної та потужної системи цивільного захисту населення і територій України потребує ще більш тісної співпраці з відповідними європейськими структурами, зокрема в рамках Механізму цивільного захисту Європейського Союзу. Главою 6 «Навколишнє природне середовище» розділу 5 «Економічне і галузеве співробітництво» Угоди про асоціацію між Україною та Європейським Союзом передбачено співробітництво у сфері цивільного захисту [217, с. 133-134].

Реалізації одного із пріоритетів євроінтеграції – приєднання України до Механізму цивільного захисту Європейського Союзу сприятиме, на думку О. Подскальної, підписання та реалізація нової редакції Адміністративної домовленості між ДСНС України та Генеральним Директоратом «Навколишнє середовище» Європейської Комісії щодо співпраці між Координаційним центром реагування на надзвичайні ситуації Механізму цивільного захисту Співтовариства та Оперативно-черговою службою ДСНС України, подальша участь у заходах Фази 2 Програми Європейського Союзу з попередження, готовності та реагування на катастрофи природного та техногенного характеру для країн Східного партнерства (PPRD East) [217, с. 134].

Отже, враховуючи євроінтеграційні прагнення України, для органів публічної адміністрації нагальним є завдання завершити адаптацію національного законодавства в частині правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності до права Європейського Союзу.

На окрему увагу заслуговує досвід організації та правового забезпечення цивільного захисту в окремих державах, які є членам Європейського Союзу.

Як зазначає В. Шойко, у структурі Федерального відомства захисту населення та допомоги при катастрофах Федерального МВС Німеччини (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) створено

централізований орган, який забезпечує координацію виконавчих, муніципальних, урядових та органів громадського захисту територій, у контексті національної безпеки.

Разом з Федеральним відомством у структурі Федерального МВС Німеччини функціонує Департамент з питань кризового менеджменту та захисту населення. Основні завдання Департаменту полягають у координації управління у цій галузі між федеральною владою та федеральними землями, вирішенні питань правового забезпечення, бюджетного фінансування та кадрової політики. У той же час вирішення ключових завдань у випадку виникнення криз чи надзвичайних ситуацій на місцевому рівні все ще належить до компетенції федеральних земель, а вирішення цих проблем забезпечують МВС земель [295, с. 371; 340, с. 257].

Слід також звернути увагу на Федеральне агентство технічної допомоги (Bundesanstalt Technisches Hilfswerk) як Федеральну робочу групу. Агентство звітує перед Федеральним МВС і виконує завдання з питань цивільного захисту. Федеральне агентство технічної допомоги на 99 % складається з добровольців (станом на 2018 р. – приблизно 75 000 учасників). Законодавством передбачено, що Федеральне агентство технічної допомоги спочатку має бути запрошене до роботи органом з безпеки (наприклад, округом, містом, чи муніципалітетом), якщо місцеві органи цивільної оборони не можуть подолати проблему.

У серпні 2016 р. уряд ФРН вперше після закінчення холодної війни представив нову Концепцію цивільної оборони [166, с. 340; 340, с. 257]. Відповідно до положень зазначеної Концепції, основою розвитку системи цивільної оборони Німеччини має бути комплексна інтегрована система механізмів державного управління запобіганню різним небезпекам та реагуванню на надзвичайні ситуації різного характеру, розроблена з використанням поточного та перспективного потенціалів цивільної оборони. Зазначена система повинна забезпечити створення умов для виживання населення та підтримання функціонування інфраструктурних об’єктів

(структур), важливих для діяльності держави та її обороноздатності [340, с. 257].

Таким чином, у Федеративній Республіці Німеччина позитивним є досвід утворення Федерального агентства технічної допомоги (Bundesanstalt Technisches Hilfswerk), яке на 99 % складається з добровольців та виконує завдання з цивільного захисту у випадках, коли основні органи публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, не справляються з ліквідацією надзвичайної ситуації.

Н. Григоренко також зазначає, що у Федеративній Республіці Німеччина основу формувань цивільного захисту складають підрозділи, що входять до Служби захисту від катастроф, загальне керівництво якими здійснює федеральний Союз самозахисту. Усього в країні функціонує більше 400 його відділень. Ці служби укомплектовано добровольцями, кожен з яких зобов'язаний пропрацювати в ній 10 років за умови, що буде звільнений від військової повинності. Чисельність особового складу служби при повному її розгортанні досягає 600 тис. осіб. Основна тактична одиниця – взвод. За необхідності можуть створюватися роти, батальйони (загони). Наприклад, у 100 районах – імовірних об'єктах ядерних ударів створено міжрайонні загони загальною чисельністю до 40 тис. осіб. У великих населених пунктах розгорнуто підрозділи, до яких входить до 100 тис. осіб. У формуваннях служби налічується також більше 11 тис. транспортних і спеціальних автомашин, є й інші технічні засоби.

До цієї служби входять або тісно співпрацюють із нею ціла низка добровільних громадських організацій: «Товариство німецького Червоного Хреста», «Робочий союз самаритян», «Німецьке суспільство порятунку життя», «Мальтійська служба допомоги», технічна допоміжна і протипожежна служби. Загальна кількість членів цих добровільних організацій і штатного особового складу – понад 1,5 млн осіб [82, с. 294; 315, с. 369-370].

Таким чином, у ФРН підрозділи, що входять до Служби захисту від катастроф, комплектуються за рахунок добровольців, які фактично проходять

альтернативну військовій службу в системі цивільного захисту. Такий позитивний досвід заслуговує на увагу та імплементацію в національне законодавство та юридичну практику. Після закінчення воєнного стану в Україні перед органами публічної адміністрації постане питання не тільки відновлення України, але й забезпечення діяльності єдиної державної системи цивільного захисту у повоєнний період, що потребуватиме значних фінансових та людських ресурсів. Тому проходження альтернативної військовій служби в системі цивільного захисту забезпечить належний мобілізаційний ресурс для ліквідації наслідків надзвичайних ситуацій, викликаних негативними чинниками повоєнного характеру (детонація снарядів та мін, які не розірвалися під час ведення бойових дій, розбір завалів після ракетних обстрілів, які матимуть місто і після встановлення умовного миру тощо).

Крім того, Н. Григоренко зазначає, що у ФРН, як і в багатьох розвинених країнах, значна увага приділяється утворенню добровільних формувань на підприємствах з чисельністю працівників від 30 і більше осіб. Таким чином, самозахист організується за місцем роботи, причому органи управління та підрозділи комплектуються добровільно [82, с. 294].

Вказаний позитивний досвід ФРН щодо залучення добровольців та добровільних формувань до ліквідації надзвичайних ситуацій та їх наслідків, організації цивільного захисту в цілому, також заслуговує на увагу та впровадження в національну юридичну практику та практику діяльності органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту.

Також Н. Григоренко звертає увагу на досвід Нідерландів у сфері організації системи цивільного захисту і зазначає, що її було створено в 1952 році. Загальне керівництво цією системою здійснює Міністерство внутрішніх справ через головне управління цивільного захисту. Для виконання рятувальних і невідкладних аварійно-відбудовних робіт у разі стихійних лих, значних виробничих аварій та катастроф у мирний час у розпорядженні

органів управління цивільним захистом зі складу збройних сил створюється так звана «рятувальна бригада», два мотопіхотних батальйони по 650 осіб, три роти – медична, інженерна, транспортна, взвод військової поліції та санітарний загін [82, с. 293].

Таким чином, в Нідерландах в процесі управління системою цивільного захисту у разі настання надзвичайної ситуації ставка робиться на військові підрозділи та їх технічні можливості.

Територію країни поділено на 12 округів (за кількістю провінцій). В окрузі цією діяльністю керує комісар провінції, а безпосереднє керівництво здійснює начальник служби цивільного захисту та його штаб. Округи поділяються на 45 районів, які віднесені до групи «А» (промислові) та групи «В» (сільськогосподарські). Райони цивільного захисту групи «А» поділено на сектори. За кожним сектором на період надзвичайних ситуацій закріплено відповідні формування цивільного захисту. Старший начальник одного з таких формувань одночасно виконує й обов'язки начальника служби цивільного захисту сектора.

Начальником служби цивільного захисту окремих громад є бургомістр. Йому підпорядковуються всі служби: протипожежна, медична, поліцейська, комунальних послуг та соціального забезпечення. Керівним органом у районі є рада, до складу якої входять бургомістри общин, начальники та штаби цивільного захисту.

Отже, в Нідерландах ключову роль в організації управління системою цивільного захисту відграють органи місцевого самоврядування.

Штаби округів та районів у мирний час укомплектовано лише командним складом і технічним персоналом, а штати військового часу можуть розгортатись лише на період навчань та у разі виникнення надзвичайних ситуацій [82, с. 293].

Окрему увагу слід звернути на позитивний досвід залучення добровольців до рятувальної справи в окремих країнах Європи на прикладі добровільної пожежної охорони.

Так, Європейська система функціонування пожежної охорони базується на пожежних підрозділах місцевих органів влади та добровільних протипожежних формуваннях. На даний час до 80% пожежних підрозділів Великої Британії, Німеччини, Франції та Італії складається з добровольців, що свідчить про ефективність можливої співпраці професійних пожежних частин з громадськими та волонтерськими організаціями в питаннях запобігання та пом'якшення наслідків від пожеж. В Європі пожежні добровольці відіграють більш вагому роль, ніж професійні пожежні [227].

У кожній країні Європи існує свій підхід до розвитку добровільної пожежної охорони. У Німеччині добровільні пожежні команди існують у понад 2070 населених пунктах. У Швейцарії і Австрії добровольці становлять понад 90% від загальної чисельності пожежників, а в Польщі налічується понад 3,8 тис. добровільних пожежних частин. Оснащення добровільних пожежних команд є не гіршим, а то навіть і кращим, ніж у професійних. Особливістю добровільної пожежної охорони країн Європи є те, що добровільні пожежники створюють громадські об'єднання (союзи, асоціації тощо) [227].

Важливим також є позитивний досвід матеріально-технічного забезпечення добровільної пожежної охорони в зарубіжних країнах.

У більшості зарубіжних країн діяльність пожежних-добровольців стимулюється певними пільгами або застосовується погодинна оплата праці (наприклад, за час чергування або за виконання певного обсягу робіт з гасіння пожеж). Крім того, у більшості країн ЄС і в США часто застосовуються засоби морального стимулювання діяльності пожежних-добровольців у вигляді різноманітних нагород, спеціальних відзнак тощо [227].

Добровільні формування в країнах Європи є місцевими центрами протипожежної пропаганди та поширення знань із пожежної безпеки. Добровольці організовують виставки, показові виступи, бесіди на протипожежну тематику [227].

Цікавим є досвід залучення приватних компаній для ліквідації надзвичайних ситуацій та їх наслідків. Так, Н. Григоренко відзначає, що в країнах Європейського Союзу системи цивільного захисту (цивільної оборони) включають у себе сили та засоби загальнодержавного, федерального (регіонального) та муніципального рівня (які утворюються та фінансуються органами місцевого самоврядування). Крім того, в країнах ЄС активно розвиваються та функціонують приватні рятувальні служби, причому їх підрозділи дислокуються та діють як на території однієї держави, так і на територіях декількох сусідніх держав. До прикладу – це приватний рятувальний корпус «Фальк» в Королівстві Данія, який наразі є найбільшою приватною рятувальною службою у Європі, що заснована на засадах приватного акціонерного товариства, є багатофункціональною та діє у Данії, Німеччині та Швеції [82, с. 295].

Крім того, важливим елементом цивільного захисту у зарубіжних країнах, на думку Н. Григоренко, є органи публічної адміністрації, які реалізують державну політику у сфері цивільного захисту щодо надання відповідної допомоги зарубіжним країнам. До прикладу – Бюро з надання допомоги зарубіжним країнам при стихійних лихах у США надає матеріальну та технічну допомогу постраждалим країнам на їх запит протягом 24-72 годин [82, с. 295-296].

Поряд з участю в заходах міжнародних організацій західні країни прагнуть розвивати двосторонні зв’язки та співпрацю з надання допомоги під час виникнення надзвичайних ситуацій, у тому числі у проведенні аварійно-рятувальних робіт, розміщенні та життєзабезпеченні постраждалих тощо. Практично між усіма західноєвропейськими державами укладено відповідні договори [82, с. 295-296; 294, с. 159-160].

Ключову роль в організації міжнародної співпраці у сфері забезпечення безпеки життєдіяльності та цивільного захисту відіграють інформаційні технології, які дозволяють здійснювати комунікацію між органами публічної адміністрації, які реалізують державну політику у сфері цивільного захисту,

різних країн та оперативно реагувати на надзвичайні ситуації національного або міждержавного рівня (наслідки яких поширюються на територію декількох держав).

Наведений зарубіжний досвід організації та матеріально-технічного забезпечення добровільної пожежної охорони заслуговує на запозичення та імплементації в національне законодавство та юридичну практику.

3.2 Особливості адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в Сполучених Штатах Америки, Канаді та Сполученому Королівстві Великої Британії та Північної Ірландії

Дослідження перспективних напрямів удосконалення національного законодавства у сфері адміністративно-правового регулювання забезпечення безпеки життєдіяльності, включаючи використання інноваційних інформаційних технологій, включає обов'язковий аналіз зарубіжного досвіду, адже цивілізовані зарубіжні країни пройшли довгий шлях формування національних систем цивільного захисту та забезпечення безпеки життєдіяльності в цілому.

Однією з найбільш розвинутих в технологічному плані країн є США, адже саме у США зародилася технологія Інтернет і органи публічної адміністрації приділяють максимальну увагу розвитку електронного урядування, цифровізації системи публічного управління в цілому.

Крім того, США в силу географічних факторів та масштабів країни достатньо часто потерпають від різноманітних природних катаклізмів, що потребує від органів публічної адміністрації підтримки рівня максимальної готовності відповідних служб для оперативного реагування на надзвичайні ситуації та високого рівня координації всіх сил та засобів для ліквідації наслідків надзвичайних ситуацій.

Україна тісно взаємодіє із США на всіх напрямах забезпечення національної безпеки, тому дослідження досвіду адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в США має як теоретичне, так і практичне значення з метою виокремлення позитивного зарубіжного досвіду у вказаній сфері суспільних відносин та визначення доцільності та необхідності його імплементації в національне адміністративне законодавство та юридичну практику.

В сучасному глобалізованому, високотехнологічному та цифровізованому світі люди все більше стикаються із новими викликами та загрозами природного та техногенного характеру. Теорія глобального потепління не є абсолютно доведеною, проте наслідки життєдіяльності людини, зокрема, активного розвитку високотехнологічного виробництва, є очевидними. Збільшення викидів парникових газів призводить до збільшення середньої температури на планеті та посилення потужності природних катаклізмів, які стають причиною виникнення надзвичайних ситуацій, тобто порушення нормальних умов життєдіяльності населення відповідних територій. Так загальновідомими є останні наслідки руйнівних лісових пожеж, ураганів, зокрема і на території США.

Вищезазначене обумовлює необхідність посилення уваги органів публічної адміністрації до системи забезпечення життєдіяльності, яка включає систему цивільного захисту населення від надзвичайних ситуацій та їх наслідків.

США є одним із світових лідерів у розвитку високотехнологічного виробництва та цифровізації суспільного життя. Водночас саме на території США останнім часом спостерігається збільшення кількості надзвичайних ситуацій, які зумовлені причинами природного та техногенного характеру. Отже, відповідні органи публічної адміністрації США набувають всебічного досвіду у сфері ліквідації надзвичайних ситуацій та їх наслідків.

Так, І. Прощин зазначає, що щодо закордонного досвіду в ліквідації наслідків надзвичайних ситуацій природного характеру, то найбільшої уваги

заслуговує досвід США – країни, в якій масштабні катастрофи природного характеру трапляються досить часто, на густонаселених територіях [291, с. 96].

Головним органом з питань запобігання та ліквідації наслідків природних і техногенних катастроф в США є FEMA (Federal Emergency Management Agency), яке створено у 1997 році. Воно координує діяльність органів цивільної оборони, федеральних міністерств та відомств (міністерств енергетики, транспорту та ін.) і підприємств приватного сектору, а також забезпечує підготовку кадрів, навчання населення та поширення інформації з питань реагування на надзвичайні ситуації, проведення науково-дослідних робіт, контроль за використанням електронних засобів масової інформації в період надзвичайного стану, взаємодію зі збройними силами [291, с. 96; 180, с. 10-12].

Як зазначено на офіційному веб-сайті FEMA, у Федеральному агентстві з управління надзвичайними ситуаціями (FEMA) працює понад 20 000 людей по всій країні. Штаб-квартира у Вашингтоні, округ Колумбія, має 10 регіональних офісів по всій країні. FEMA використовує величезний потенціал для координації в рамках федерального уряду, щоб переконатися, що Америка готова до катастроф і реагує на них [357].

Місія FEMA полягає в тому, щоб допомагати людям до, під час і після катастроф. Цілі та завдання FEMA, викладені в Стратегічному плані на 2022-2026 роки, покликані забезпечити успіх агентства, спільноти з управління надзвичайними ситуаціями. План окреслює три сміливі амбітні цілі для вирішення цього завдання:

- впроваджувати справедливість як основу управління надзвичайними ситуаціями;

- очолювати всю спільноту в боротьбі зі змінами клімату;

- підтримувати готовність FEMA та підготовлену націю [357].

Слід відзначити, що важливу роль в координації діяльності регіональних офісів FEMA відіграють новітні інформаційні технології. Зокрема на

вказаному офіційному сайті FEMA доступна всебічна інформація про діяльність агентства, освітні програми, останні надзвичайні події (ситуації) та заходи реагування на них, Стратегічний план на FEMA на 2022-2026 роки, інформація про основні ризики природного та техногенного характеру та заходи щодо їх своєчасного виявлення та запобігання негативним наслідкам тощо.

Акумулювання інформації про надзвичайні ситуації забезпечується засобами комунікації з використанням новітніх інноваційних інформаційних технологій: швидкісного оптоволоконного зв'язку, захищеного серверного обладнання, хмарних технологій, можливостей соціальних мереж та месенджерів, технології штучного інтелекту тощо.

Комплексний характер системи державного управління США щодо надзвичайних ситуацій відображають наступні принципи: координація діяльності органів управління, що відповідальні за підготовку і протидію надзвичайним ситуаціям, з боку однієї особи (директора FEMA), підлеглої безпосередньо президенту США; подвійне призначення, тобто об'єктами управління є надзвичайні ситуації мирного та воєнного часу, а суб'єктами управління – цивільні та військові організації; надзвичайні повноваження відповідних органів управління повинні бути продовженням їх звичайних, повсякденних функцій там, де це можливо; взаємозв'язок між всіма фазами (функціями) управління [291, с. 96; 232, с. 275].

Реалізація зазначених принципів в США дозволила побудувати ефективну систему цивільного захисту населення та територій від надзвичайних подій природного та техногенного характеру.

В. Панфілов зазначає, що комплексний характер державної системи управління щодо надзвичайних ситуацій, захисту населення від техногенних аварій та катастроф у США проявляється у створенні всеохоплюючої системи федерального законодавства, що регулює практично всі етапи розвитку техногенно-екологічної безпеки [200, с. 30].

Особливість правового регулювання суспільних відносин в США як федеративній державі обумовлює наявність двох рівнів законодавства: федерального та законодавства штатів. Проте, враховуючи особливе значення для суспільства правової регламентації організації цивільного захисту, ключові питання техногенно-екологічної безпеки, тобто захисту населення та територій від надзвичайних ситуацій природного та техногенного характеру вирішуються на рівні саме федерального законодавства.

Р. Приходько та О. Ященко акцентують увагу на тому факті, що у системі адміністративно-правового регулювання захисту населення і територій від надзвичайних ситуацій у США має місце розподілення функцій і повноважень (FEMA виконує лише частину з них, консолідуючи зусилля органів державного управління, що здійснюють іншу частину обов'язків). Так, питаннями прогнозування й оцінки ризику надзвичайних ситуацій займається Національна служба погоди, ризику повені – Національна адміністрація по океанографії і метеорології; ризику землетрусів – Національний науковий фонд та геологічна служба США; розробкою стандартів і нормативів будівництва укріплювальних споруд – Інженерні війська США та Національне бюро стандартів. Відповідно, через вищезазначені органи FEMA отримує повідомлення про катастрофи. Також аналогічна інформація надходить з правоохоронних органів, оперативного центру комісії з атомного законодавства, місцевого оперативного центру з питань надзвичайних ситуацій, агентства новин США [232, с. 276-277].

Таким чином, головним завданням FEMA є саме координація діяльності органів публічної адміністрації щодо своєчасного реагування на надзвичайні ситуації та оперативної ліквідації їх негативних наслідків, а також акумулювання інформації про надзвичайні ситуації, що забезпечується засобами комунікації з використанням інноваційних інформаційних технологій (швидкісного оптоволоконного зв'язку, серверного обладнання, хмарних технологій, можливостей соціальних мереж та месенджерів тощо).

Після отримання першого повідомлення про катастрофу, FEMA через національний центр координації надзвичайних ситуацій повідомляє свої філії і регіональні офіси, а також групу надання допомоги при катастрофах і бригаду невідкладного забезпечення. Отримавши підтвердження про розмір руйнувань і людських жертв від губернатора постраждалого штату, директор FEMA направляє запит до Білого дому про оголошення в районах, які зазнали ураження, надзвичайного стану і введення в дію Федерального плану [232, с. 277].

На підставі подання FEMA і петиції губернатора Президент США видає спеціальний указ про введення надзвичайного стану і надання федеральної допомоги штату (штатам), який постраждав. Лише у виняткових випадках згідно з законодавством Президент може ввести надзвичайний стан у штаті без петиції губернатора. Після цього FEMA посилає у зону лиха свого координатора, даючи вказівки щодо розгортання формувань і установ в осередку та за його межами. У відповідності з Федеральним планом та конкретними заявками постраждалих штатів головні відомства й агентства спрямовують виділені сили і засоби для ліквідації наслідків катастрофи (після їх коригування на центральному рівні). FEMA здійснює фінансове відшкодування витрат на ліквідацію катастрофи відповідно до законодавства (Financial Management Annex and Regulations in 44 CFR part 206). Подальша робота здійснюється при прямому контакті штаб-квартири FEMA зі своїми регіональними офісами, федерального координатора з координаторами штатів, національних міністерств і агентств зі своїми відділами і філіями у постраждалих штатах. Крім того, здійснюється співробітництво FEMA з усіма головними відомствами (міністерствами, агентствами) і основними формуваннями, що працюють в осередку [232, с. 277].

О. Сохін справедливо зазначає, що в окресленій системі позитивним моментом є визначення субординації, розподіл обов'язків усіх організацій-учасників і визначення механізму їх взаємодії. Певним недоліком, на його думку, можна вважати надто велику кількість міністерств, відомств, агентств,

установ і тимчасових формувань, які беруть участь у ліквідації наслідків катастрофи [301, с. 32].

Проте вказаний недолік цілком компенсується координаційними зусиллями FEMA, що діє у відповідності до єдиного Федерального плану.

В. Домański зазначає, що, оскільки питання про взаємодію органів в США повинні розв'язувати задовго до інциденту, у Портленді створено групу розвитку і планування, яка співпрацює з представниками промислових підприємств і добровільних формувань [87, с. 31].

Зазначений позитивний досвід вартий запозичення та імплементації в національне законодавство та юридичну практику, адже в умовах ринкової економіки та розвинутого громадянського суспільства представники промислових підприємств, підприємці в цілому та добровільні формування повинні бути однією з основних ланок загальнодержавної системи цивільного захисту, адже вони максимально наближені до місць потенційного виникнення надзвичайних ситуацій та здатні вчинити першочергові (невідкладні) дії щодо ліквідації надзвичайної ситуації та локалізації її наслідків.

Ключовою є також ефективна комунікація з представниками промислових підприємств і добровільних формувань, яку доцільно здійснювати із використанням новітніх інформаційних технологій, що дозволить оперативно реагувати на виникнення чи загрозу виникнення надзвичайної ситуації.

Разом із тим, форми та методи адміністративно-правового регулювання зазначеною сферою в США, на думку Р. Приходько та О. Ященко, надто громіздкі та важко керовані з єдиного центру, втім у такому регулюванні захисту населення і територій від надзвичайних ситуацій є також позитивні моменти, а саме: FEMA керується тільки одним Федеральним планом, який є головним актом у процесі реагування на надзвичайну ситуацію та ліквідацію її наслідків. За результатами проведеного дослідження науковці запропонували розробити найбільш загальний національний план реагування на надзвичайні ситуації різного характеру, в якому прописати – які

міністерства та відомства будуть брати участь у ліквідації наслідків надзвичайної ситуації техногенного та природного характеру. І лише на підставі загального плану розробляти плани для окремих районів, з урахуванням їх особливостей [232, с. 277-278].

Таким чином, загальний федеральний план реагування на надзвичайні ситуації різного характеру дозволяє оперативно розробляти актуальні плани реагування на конкретну надзвичайну ситуацію на регіональному або на загальнодержавному рівні.

Не менш важливе значення для подолання наслідків надзвичайних ситуацій мають програми, які спрямовані на захист прав і свобод громадян в умовах надзвичайної ситуації.

Б. Данилишин зазначає, що в США існують програми соціального захисту громадян шляхом надання субсидій, компенсацій, матеріальної, фінансової, медичної, гуманітарної та іншої допомоги, що сприяє нормалізації обстановки в районах надзвичайної ситуації. У законодавчому полі США чинними є «Закон про компенсацію збитків від великих аварій на АЕС», «Закон про охорону здоров'я та техніку безпеки на вугільних шахтах», «Закон про безпеку на виробництві та охорону здоров'я в гірничій справі» [88, с. 222].

Отже, система забезпечення безпеки життєдіяльності та цивільного захисту у США має належну правову основу на рівні федерального законодавства. І вже на основі федеральних законів розробляється федеральний план реагування на надзвичайні ситуації.

Так, головною метою агентства (FEMA) є розробка комплексної системи заходів у сфері захисту населення і територій від надзвичайних ситуацій. Ця система включає розробку форм та методів, стратегії однаково придатної для управління країною як при стихійних лихах, так і техногенних аварій антропогенного походження та, крім того, інтеграцію дій на рівні штатів і місцевих органів влади. І саме під егідою агентства розроблений і затверджений Федеральний план заходів стосовно ліквідації осередків катастроф (The Federal Response Plan), де закріплені принципи, організаційні

структури та стратегія управління країною як при стихійних лихах, так і при аварійних ситуаціях техногенного характеру. У підготовці цього плану брали участь 27 міністерств, агенств і комітетів національного рівня. План вводиться в дію відповідно до законодавчого акту Роберта Стаффорда про надання допомоги при надзвичайних ситуаціях (щодо невідкладної допомоги при катастрофах) [365]. На підставі загального Федерального плану складаються відомчі, регіональні та місцеві плани невідкладних заходів. Крім того, визначаються механізми реалізації різних видів допомоги постраждалому штату. У разі виникнення декількох надзвичайних ситуацій у різних штатах вводиться в дію план одночасного надання допомоги штатам, що постраждали (Multi-State Response Operations) [301, с. 31].

Вищевказаний досвід США щодо розробки та реалізації єдиного Федерального плану реагування на надзвичайні ситуації запозичений національними органами публічної адміністрації та імплементований в національне законодавство та відповідну юридичну практику. Так, постановою Кабінету Міністрів України від 14 березня 2018 р. № 223 затверджено План реагування на надзвичайні ситуації державного рівня [244].

Зазначений План реагування на надзвичайні ситуації державного рівня розроблено для впорядкування та координації дій органів державної влади України, органів місцевого самоврядування, органів управління та сил цивільного захисту, суб’єктів господарювання, спрямованих на ліквідацію наслідків та надання допомоги постраждалим, у разі загрози виникнення або виникнення надзвичайної ситуації [244].

Ліквідацією наслідків надзвичайних ситуацій природного характеру у США займаються громади та органи влади населених пунктів, адміністративних територій, штатів. У випадках, коли місцева громада, адміністративна територія чи навіть штат не в силах протидіяти надзвичайній ситуації, терміново запрошується допомога Федерального Уряду і починає діяти Національна система захисту населення та територій від надзвичайних ситуацій. На державному рівні дії системи детально плануються у Плані

федерального реагування, а на регіональному – дії, сплановані у Планах реагування конкретного штату, регіону, району. Концепція реалізації Планів полягає в тому, що при надзвичайних ситуаціях після отримання інформації з місця катастрофи, негайно вступає в дію Регіональний план. До місця катастрофи висуваються регіональні мобільні елементи реагування: пожежники, поліція, бригади швидкої медичної допомоги, які формують біля місця катастрофи командний пункт. Починається виконання обов'язків рятувальниками кожного напрямку і водночас детальна розвідка наслідків катастрофи та її поширення. Інформація подається в центр зв'язку, дається оцінка обставин, розміру санітарних втрат, стану небезпеки для населення і перші прогнози щодо потреб додаткових сил. За необхідності губернатор штату направляє сили та засоби, які він має згідно з Регіональним планом, доповідає про катастрофу та її наслідки Федеральному агентству боротьби з надзвичайними ситуаціями і за необхідності просить допомоги. Федеральний уряд в цьому разі негайно приймає відповідальність за управління всіма діями щодо реагування на катастрофу і вводить в дію Федеральний план [291, с. 96; 180, с. 11-12].

О. Сохін зазначає, що федеральний план передбачає надання допомоги, спрямованої, насамперед, на порятунок життя людей, захист установ громадської охорони здоров'я і власності, забезпечення національної безпеки. Він не стосується будівництва житла, позик і грантів, наданих окремим громадянам і місцевій адміністрації для остаточної ліквідації наслідків катастрофи [291, с. 96-97; 301, с. 31-32].

Отже, адміністративно-правове регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в США здійснюється як на рівні федерального законодавства, так і на рівні законодавства штатів. Ключовим органом публічної адміністрації, який здійснює нормотворчу діяльність у вказаній сфері суспільних відносин є Федеральне агентство з управління надзвичайними ситуаціями – FEMA (Federal Emergency Management Agency), яке координує діяльність органів цивільної оборони,

федеральних міністерств та відомств (міністерств енергетики, транспорту тощо) і підприємств приватного сектору, а також забезпечує підготовку кадрів, навчання населення та поширення інформації з питань реагування на надзвичайні ситуації.

На окрему увагу заслуговує організація забезпечення безпеки життєдіяльності та цивільного захисту в США на регіональному рівні, а також організація інформаційної взаємодії між різними органами публічної адміністрації та інститутами громадянського суспільства в процесі ліквідації надзвичайних ситуацій, включаючи питання використання інформаційних технологій.

Так, як зазначає А. Остап'юк, система цивільного захисту в США є великою та комплексною, яка охоплює різні рівні управління та агентства, діяльність яких спрямована на запобігання, реагування та відновлення в разі надзвичайних ситуацій. Найважливішим органом в цій системі є Федеральне управління надзвичайними ситуаціями (Federal Emergency Management Agency, FEMA). У додаток до FEMA, національна система цивільного захисту включає державні та місцеві управління з надзвичайних ситуацій, а також різноманітні агентства та організації, які виконують різні функції у цій сфері. Кожен штат має своє власне управління з надзвичайних ситуацій, яке відповідає за планування та реагування на катастрофи на рівні штату, а також співпрацює з FEMA у разі потреби у федеральній допомозі. Система цивільного захисту також передбачає міжагентурну співпрацю між різними органами уряду, а також громадськими та приватними організаціями. Це сприяє ефективному обміну інформацією та ресурсами під час кризових ситуацій. Важливою складовою цієї системи є також громадська свідомість та підготовка. Освіта та навчання громадськості про правила поведінки в разі надзвичайних ситуацій, а також підготовка сімей та спільнот до реагування на кризові ситуації, безумовно, є ключовими елементами успішного функціонування системи цивільного захисту в США [196, с. 91].

Також А. Остап’юк зазначає, що для забезпечення належного функціонування системи цивільного захисту в США управління при виникненні надзвичайних ситуацій відбувається через Національний центр координації реагування FEMA (NRCC). NRCC є міжвідомчим центром, який розташований у штаб-квартирі FEMA і здійснює координацію загальної федеральної підтримки ліквідації великих катастроф і надзвичайних ситуацій, а також забезпечує підтримку операцій на регіональному рівні. Керівник FEMA активує роботу NRCC при виникненні надзвичайної ситуації шляхом координації роботи персоналу. NRCC координує роботу з постраждалими регіонами та надає необхідні ресурси та політичні вказівки для підтримки операцій на регіональному рівні. Персонал NRCC забезпечує координацію управління надзвичайними ситуаціями, планування, розгортання ресурсів, а також збирає та розповсюджує інформацію про інциденти, формуючи та підтримуючи обізнаність про ситуацію на національному рівні [196, с. 91-92].

Таким чином, Національний центр координації реагування FEMA (NRCC) є ключовим міжвідомчим центром, який забезпечує накопичення та опрацювання інформації про надзвичайні ситуації та їх наслідки, а також здійснює координацію діяльності інших органів публічної адміністрації з метою ліквідації надзвичайних ситуацій, чому сприяє високий рівень цифровізації органів публічної адміністрації в США, забезпечення їх якісним інтернетом та мобільним зв’язком.

Крім того, А. Остап’юк наводить статистику, згідно з якою в США на даний час діє понад 6 тис. диспетчерських центрів, які обслуговують виклики на номер 911. Більшість з них оснащені спеціальним обладнанням, яке автоматично відображає номер та адресу абонента на дисплеї оператора в момент надходження дзвінка. Це значно спрощує процес реагування на надзвичайні ситуації, особливо у випадках, коли абонент має проблеми з мовою або не може говорити. При надходженні дзвінка до диспетчерського центру, оператор відповідає на нього протягом кількох секунд та називає свій ідентифікаційний номер. Абонентові рекомендується запам’ятати цей номер,

якщо у нього виникнуть проблеми з обслуговуванням або якщо пізніше потрібно буде звернутися за додатковою інформацією. Оператор задає різні запитання, відповіді на які допомагають класифікувати дзвінок залежно від ситуації. Ці дані вводяться в спеціальну комп'ютерну систему, яка визначає найближчий ресурс, який може відправитися на місце події негайно [82; 196, с. 92].

Таким чином, сучасні інформаційні технології дозволяють оперативно реагувати на надзвичайні події, використовуючи цифрові інструменти визначення геолокації інциденту та пов'язуючи місцезнаходження епіцентру надзвичайної ситуації із місцезнаходженням найближчих сил та засобів цивільного захисту.

Важливе значення для ефективного функціонування системи цивільного захисту в США має організація діяльності регіональних органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту. Так, А. Остап'юк зазначає, що на регіональному рівні в США важливий акцент робиться на забезпеченні ефективної координації та реагування на надзвичайні ситуації в межах конкретного регіону. Одним із ключових аспектів є наявність місцевих управлінь з надзвичайних ситуацій, які відповідають за розробку та виконання планів підготовки та реагування на надзвичайні ситуації відповідно до специфічних потреб та умов свого регіону. Основна мета регіональних органів управління надзвичайними ситуаціями полягає в ефективному координуванні дій різних агентств та ресурсів на місцевому рівні. Це включає управління пожежною охороною, медичними службами, правоохоронними органами, волонтерськими групами та іншими зацікавленими сторонами для забезпечення швидкого та ефективного реагування на будь-які небезпечні ситуації. Крім того, на регіональному рівні активно впроваджуються програми підготовки та навчання громадськості щодо дій в разі виникнення надзвичайних ситуацій. Ці програми спрямовані на підвищення обізнаності та готовності населення до реагування на різні загрози та кризові ситуації, що можуть виникнути на регіональному рівні.

Також важливим аспектом є розвиток і використання сучасних інформаційних технологій. Це включає системи автоматизованого попередження про надзвичайні ситуації, моніторинг погодних умов та інших потенційних загроз, а також використання мобільних додатків та інтернет-ресурсів для розповсюдження важливої інформації та інструкцій для громадськості [196, с. 92-93].

Таким чином, сучасні інформаційні технології відіграють ключову роль в процесі функціонування системи цивільного захисту в США і відповідний позитивний досвід використання автоматизованих систем попередження про надзвичайні ситуації, моніторингу погодних умов та інших потенційних загроз, а також досвід використання мобільних застосунків та інтернет-ресурсів для розповсюдження важливої інформації та інструкцій для громадян заслуговує на запозичення та імплементацію в національне законодавство та практику організації цивільного захисту.

В якості позитивного прикладу використання сучасних інформаційних технологій у сфері цивільного захисту можна навести офіційний веб-сайт Геологічної служби США – https://www.usgs.gov/. На вказаному сайті особа може не тільки ознайомитися із поточним станом геологічної активності Землі, але й ознайомитись із науковими прогнозами щодо можливої сейсмічної активності в певних регіонах та підготуватись до потенційних надзвичайних ситуацій.

Серед позитивних моментів досвіду США щодо забезпечення ефективного функціонування системи цивільного захисту А. Остап’юк виділяє наступні:

- система цивільного захисту в США є дуже гнучкою та адаптивною, що дозволяє швидко реагувати на різноманітні надзвичайні ситуації на регіональному рівні. Місцеві управління з надзвичайних ситуацій мають можливість реагувати згідно з конкретними потребами та характеристиками своєї місцевості;

- важливим елементом успішної системи цивільного захисту США, в тому числі й на регіональному рівні, є співпраця між різними органами та агентствами, як на загальнодержавному, так і міжнародному рінях. Це включає урядові агентства, правоохоронні органи, медичні служби, пожежну охорону, а також громадські та приватні організації;

- США мають розвинуту систему підготовки та навчання населення щодо дій в разі виникнення надзвичайних ситуацій, що включає регулярні тренування, проведення кампаній з громадської освіти та інформаційних кампаній щодо підготовки до різних видів кризових ситуацій;

- використання сучасних технологій. В процесі діяльності різних органів держави важливу роль відіграють сучасні технології, такі як системи автоматизованого попередження про надзвичайні ситуації, мобільні додатки для інформування громадян. Всі вони активно використовуються з метою покращення ефективності системи цивільного захисту на регіональному рівні [196, с. 93].

Таким чином, вартими запозичення є такі елементи позитивного досвіду США у сфері забезпечення безпеки життєдіяльності та цивільного захисту як використання сучасних інформаційних технологій для автоматизованого попередження про надзвичайні ситуації, а також використання мобільних застосунків для інформування громадян.

Не менш позитивним є позитивний досвід США щодо залучення добровільних громадських формувань для ліквідації надзвичайних ситуацій та їх наслідків.

Так, Н. Григоренко зазначає, що важливу роль у системі цивільного захисту США відіграють громадські формування, зокрема добровільна організація «Громадський військовий патруль» (об’єднує власників приватних літаків), американський Червоний Хрест, товариство «Армія Спасіння» (благодійна організація) тощо. Особлива роль у ліквідації наслідків стихійних лих, аварій, катастроф належить національній гвардії (організований резерв збройних сил США). Її підрозділи перебувають у підпорядкуванні

губернаторів штатів і використовуються для підтримки громадського порядку, забезпечення нормального функціонування урядових установ, ліквідації наслідків стихійних лих і вирішення інших завдань [82, с. 292].

Крім того, Н. Григоренко також відзначає, що ключову роль в організації взаємодії між органами публічної адміністрації, які реалізують державну політику США у сфері цивільного захисту, та громадськими формуваннями відіграють інформаційні технології, які забезпечують ефективну комунікацію між підрозділами FEMA та іншими суб'єктами американської системи цивільного захисту. Так, застосування інтернет-ресурсів та мобільних застосунків дозволяє оперативно інформувати громадські формування та окремих активістів-добровольців про надзвичайні ситуації, місце та час їх виникнення, масштаби негативних наслідків та необхідні сили та засоби цивільного захисту для ліквідації вказаних надзвичайних ситуацій [82, с. 292-293].

Окрему увагу Н. Григоренко приділяє досвіду побудови систем надання державних послуг у сфері цивільного захисту в Канаді і зазначає, що цивільний захист Канади як система захисту населення, економіки й адміністративно-політичної структури функціонує з 1957 року. Відповідальність за вирішення завдань цивільного захисту покладається на прем'єр-міністра, який призначає одного з міністрів Федерального уряду відповідальним за надзвичайну готовність. Діяльність усіх міністрів координується Агентством надзвичайної готовності Канади (EPC), яке очолює виконавчий директор, що має заступника з планування й оперативного управління. Територію країни поділено на 10 округів надзвичайної готовності. Спеціальних формувань у системі цивільного захисту в Канаді немає, а до вирішення завдань цивільного захисту залучаються поліція, пожежна служба, медичні установи, військові підрозділи. В умовах надзвичайної ситуації на їхній основі, у разі потреби, формуються мобільні рятувальні групи для дій у районах надзвичайних ситуацій [82, с. 293].

Таким чином, в Канаді відсутні спеціальні формування у системі цивільного захисту, проте налагоджена система формування мобільних рятувальних груп із залученням представників поліції, пожежної служби, медичних установ та військових підрозділів. Мобілізації сили та засобів цивільного захисту сприяє розвинута система інформаційної взаємодії між центральними органами публічної адміністрації та переліченими вище підрозділами на місцях [82, с. 292-293].

Таким чином, в організації механізму забезпечення життєдіяльності та цивільного захисту в Канаді ключову роль відіграють інформаційні технології, які забезпечують інформаційну взаємодію між центральними органами публічної адміністрації та підрозділами різних служб на місцях.

На увагу заслуговує також досвід організації та правового забезпечення функціонування системи цивільного захисту та механізму забезпечення безпеки життєдіяльності у Великобританії.

Як зазначає В. Шойко, загальне управління система захисту людей і територій від надзвичайних ситуацій у Великобританії забезпечує Міністерство внутрішніх справ через відповідні управління та міжміністерський плановий комітет, який координує діяльність міністерств і відомств [58, с. 32; 340, с. 255].

Відповідно до законодавства, міністр внутрішніх справ Великобританії несе загальну відповідальність за забезпечення безпеки населення, запобігання та реагування на надзвичайні ситуації та кризи. Міністр очолює спеціальний комітет Кабінету Міністрів, до складу якого входять керівники інших ключових міністерств та відомств (міністр охорони здоров'я, відповідальний за реагування на виникнення епідемій тощо). Повсякденна робота з планування, координації та підвищення ефективності діяльності органів державної влади з усього спектру надзвичайних ситуацій проводиться спеціальним секретаріатом Кабінету Міністрів [315, с. 373; 340, с. 256-257].

На місцевому рівні реалізація основних заходів організовується радами графств адміністративних округів, муніципалітетів міст через спеціально

створені комітети, які у випадку надзвичайної ситуації об'єднуються в округи й підокруги цивільної оборони та співпрацюють з військовим командуванням своєї країни та членів НАТО. Зокрема, система оповіщення у Великобританії об'єднується з системою оповіщення оперативного центру Атлантичної зони протиповітряної оборони НАТО [315, с. 373; 340, с. 256-257].

Таким чином, в процесі організації цивільної оборони у Великобританії використовуються сили та засоби Північноатлантичного альянсу (НАТО), включаючи цифрові технології систем оповіщення та реагування на надзвичайні ситуації.

Також В. Шойко зазначає, що система захисту населення та територій від різних видів надзвичайних ситуацій у Великобританії не має власних сил і засобів, за винятком корпусу спостереження, призначеного для радіаційної розвідки та дозиметричного контролю, який став основою формування національної системи спостереження за радіаційною обстановкою. У той же час військово-політичне керівництво країни докладає максимум зусиль для підготовки населення до реагування на надзвичайні ситуації та для розвитку умінь кваліфікованого персоналу у сфері запобігання та усунення їх негативних наслідків, справедливо вважаючи, що це дозволить якомога швидше привести в дію відповідні підрозділи аварійно-рятувальних робіт [315, с. 372; 340, с. 255].

У відповідності до законодавства Сполученого Королівства Великої Британії та Північної Ірландії реагування на надзвичайні ситуації відбувається на двох рівнях: національному та регіональному. На національному рівні відбувається планування дій з ліквідації надзвичайних ситуацій, пов'язаних з актами терористичної діяльності, початком збройного конфлікту, загрозами ядерного, хімічного, чи радіологічного забруднення всієї держави або окремих регіонів.

У цьому випадку розпочинає свою діяльність спеціальний урядовий комітет COBRA («Cabinet Office Briefing Room A»), який є найвищим органом, що приймає рішення у кризових ситуаціях. До складу спеціального урядового

комітету COBRA входять: міністр внутрішніх справ, начальники контррозвідки (MI 5), поліції, галузевих міністерств та відомств, члени спеціального секретаріату Кабінету Міністрів Сполученого Королівства, координатор Кабінету Міністрів з питань безпеки та розвідки тощо. Як правило, на засіданнях цього комітету головує Прем'єр-міністр Великобританії [315, с. 372-373; 324, с. 66].

Таким чином, спеціальний урядовий комітет КОБРА здійснює мобілізацію людських та матеріально-технічних ресурсів у випадку виникнення надзвичайної ситуації загальнодержавного рівня і здійснює координацію діяльності інших органів публічної адміністрації з метою забезпечення безпеки життєдіяльності.

У разі виникнення надзвичайних ситуацій та криз у регіонах, реагування на них та усунення їх наслідків доручаються: відповідним органам публічної адміністрації, службам (пожежним, поліцейським, військовим, медичним, екологічним, дорожнього нагляду тощо), урядовим офісам на місцях (де створюються відповідні спеціалізовані групи) та місцевим органам влади. До цієї роботи також активно залучається приватний сектор, який володіє мережами електро- та водопостачання, телефонними та телекомунікаційними станціями, лініями електропередач, надає транспортні та інші послуги, а також добровільні громадські організації [315, с. 373; 340, с. 256-257].

Таким чином, позитивним є досвід Великобританії щодо залучення до ліквідації надзвичайних ситуацій приватного сектору, який володіє мережами електро- та водопостачання, телефонними та телекомунікаційними станціями, лініями електропередач, надає транспортні та інші послуги, а також добровільних громадських організацій.

На увагу заслуговує також досвід адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в країнах Близького та Далекого Сходу.

3.3 Адміністративно-правові засади забезпечення безпеки життєдіяльності та цивільного захисту в країнах Близького та Далекого Сходу в умовах цифровізації

Національна система забезпечення безпеки життєдіяльності та цивільного захисту проходить важкі випробування в умовах воєнного стану, адже окрім повсякденної готовності до надзвичайних ситуацій техногенного та природного характеру Державна служба України з надзвичайних ситуацій виконує важку роботу з ліквідації наслідків ракетних та бомбових ударів по цивільній інфраструктурі.

В таких складних умовах важливе значення має пошук актуальних напрямів удосконалення публічного управління системами цивільного захисту та безпеки життєдіяльності в цілому з урахуванням позитивного зарубіжного досвіду та останніх досягнень у сфері інформаційних технологій.

Одним із світових лідерів у сфері цифровізації, розвитку та впровадження інноваційних інформаційних технологій у сферу публічного управління є Японська Держава. За останні десятиріччя Японія здійснила технологічний стрибок та по праву вважається еталоном якості та ефективності у сфері використання інформаційних технологій.

Водночас в силу свого географічного розташування Японська Держава часто потерпає від катастрофічних землетрусів та пов’язаних із ними цунамі, що обумовлює активний розвиток японської системи цивільного захисту та забезпечення безпеки життєдіяльності громадян. Водночас функціонування вказаної системи потребує належного правового врегулювання, що знаходить своє відображення у відповідному розділі японського законодавства.

Враховуючи вищезазначене, дослідження досвіду органів публічної адміністрації Японської Держави у сфері публічного адміністрування та адміністративно-правового регулювання систем забезпечення безпеки життєдіяльності та цивільного захисту в умовах цифровізації має як теоретичне, так і практичне значення в контексті необхідності запозичення

позитивного зарубіжного досвіду публічного управління у вказаній сфері суспільних відносин та визначення доцільності його імплементації в національне законодавство та юридичну практику.

Японія з точки зору юриспруденції та науки державного управління є унікальною державою, адже її правова система та організація публічного управління засновані на правових традиціях та звичаях, чим обумовлюється високий рівень правової культури та правосвідомості громадян. Таким чином, дотримання норм японського законодавства забезпечується більшою мірою внутрішнім переконанням та традиціоналізмом, аніж загрозою покарання.

Відповідно і у сферах забезпечення безпеки життєдіяльності та цивільного захисту японці проявляють внутрішню організованість та постійну готовність до навчання, злагодженість у діях та дисциплінованість.

Не менше значення для ефективного запобігання та оперативної ліквідації надзвичайних ситуацій та їх наслідків в Японській Державі має високий рівень інформатизації та автоматизації систем оповіщення населення про загрозу катастроф природного та техногенного характеру.

Д. Дубов, М. Ожеван, А. Баровська зазначають, що природні катастрофи (землетруси та цунамі) в Японії, які згодом доповнила техногенна катастрофа (атомна), стали випробуванням системи раннього сповіщання та автоматичного відключення, радикально оновленої на базі новітніх ІКТ (інформаційно-комунікаційних технологій) після 1995 року, коли стався надпотужний землетрус в регіоні префектури Кобе. В цілому ця система витримала іспит і багато в чому є взірцевою для інших країн: вона дозволила мінімізувати жертви серед населення [101].

В цьому сенсі японська система раннього сповіщення, що була введена в дію у 2007 році, і яка являє собою систему датчиків і метеорологічних станцій, розташованих на території всієї країни, яка автоматично видає попередження про землетрус, продемонструвала свою ефективність. Сейсмічні датчики фіксують первинні слабкі коливання, на підставі яких можна прогнозувати силу подальших поштовхів, і, якщо передбачувана

магнітуда буде близько п’яти, автоматично включається система оповіщення у відповідному районі. Оповіщення на стадії слабких коливань дасть громадянам, принаймні, кілька секунд, щоб зорієнтуватися в ситуації. За цей час: екстрено зупиняється транспорт; на всі телефони абонентів йде широкомовне повідомлення про те, що необхідно рятуватися, оскільки наближається землетрус; зупиняються виробництва; за 30 секунд відключається електроенергія в містах схильних до удару [101].

Таким чином, саме комплексне використання інформаційних технологій дозволяє вчасно поінформувати громадян про небезпеку, а також забезпечити автоматичне припинення функціонування комунікацій, які можуть бути зруйновані природніми катаклізмами з негативними наслідками для людей (наприклад, у випадку несвоєчасного відключення електроенергії можливі короткі замикання та як наслідок – пожежі та пошкодження обладнання).

Д. Дубов, М. Ожеван, А. Баровська підкреслюють, що в японській системі раннього сповіщення все діє максимально автоматично і не вимагає втручання людини. На те, щоб запровадити систему раннього сповіщення, Японія витратила з 1995 до 2007 р. близько мільярда доларів. Всі телефони повинні підтримувати систему оповіщення. Для туристів та відвідувачів Японії на сайтах з метеорологічної ситуації, зокрема Japan Meteorological Agency, англійською мовою поряд зі звичайним прогнозом погоди надається інформація щодо сейсмологічного стану в країні, наближення цунамі, штормів та ін.

Наслідком функціонування системи стало те, що, наприклад, у Токіо за хвилину до удару всі дзвінки перервалися, мільйони телефонів отримали повідомлення про те, що через хвилину буде землетрус і необхідно вжити заходів з порятунку життя. На всі підприємства надійшли тривожні автоматичні дзвінки або листи, заводи в екстреному режимі зупиняли лінії. Транспорт, зокрема метрополітен, також зупинявся, пасажирам повідомляли про загрозу землетрусу. Попереджувальний сигнал звучить і на вулицях, де встановлені спеціальні репродуктори, і в магазинах [101].

Отже, органи публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, повинні використовувати всі можливості мобільного зв'язку та взаємодіяти з усіма приватними мобільними операторами. Так, за допомогою мобільного зв'язку можна не тільки здійснювати екстрене оповіщення громадян про загрозу або початок надзвичайної ситуації, але й мобілізувати потенційних добровольців для ліквідації наслідків надзвичайної ситуації, враховуючи їх місцерозташування за допомогою спеціального мобільного застосунку та електронної бази даних добровольців.

З метою роз'яснення населенню наслідків катастрофи та поточного стану із її вирішення, в Японії активно задіюється національне телебачення NHK, зокрема, під час цього землетрусу система дала сигнал заздалегідь: в автоматичному режимі вона розрахувала силу землетрусу (первинні дані 8,1 бала), на розрахунок районів, схильних до удару, пішло 8,7 секунди. Більшість територій мало мінімум близько однієї хвилини і цей час пішов на те, щоб попередити населення. Всі засоби інформації в Японії орієнтовані на те, щоб доносити інформацію в реальному режимі часу. Національне телебачення в прямому ефірі показувало все, що відбувається з японською атомною станцією, постійно давало коментарі уряду та інших служб. Моментальне поширення інформації сприяло тому, що у суспільстві не поширювались чутки і панічні настрої. Під час прямого включення з диктором, який зачитував дані японської метеорологічної служби, вказувались райони, де удар буде найбільшим. Працювала також система оповіщення на комп'ютері, де вказувався навіть приблизний час до поштовхів [101].

Отже, окрім використання можливостей операторів мобільного зв'язку, необхідна взаємодія з усіма надавачами послуг цифрового телебачення та Інтернет, включаючи компанії, які надають послуги потокового мультимедіа безпосередньо споживачам (наприклад, Megogo, Sweet.tv тощо). Незалежно від того, яким застосунком користується споживач, він має отримувати екстрені повідомлення в режимі реального часу.

Позитивним є також досвід Японської Держави щодо проведення тренінгів із населенням у сфері цивільного захисту з використанням інформаційних технологій.

Так, у багатьох містах в Японії встановлено тренажери, які моделюють землетрус і показують, що відбувається в приміщенні, чого варто остерігатися і як себе поводити [101].

Не менш важливим є позитивний досвід Японії щодо проведення пошукових робіт в умовах надзвичайної ситуації.

Зокрема, під час останніх природних катаклізмів крім традиційних форм пошуку загиблих та зниклих безвісті, активно задіювались можливості соціальних мереж та новітніх інформаційних технологій. Всі японські оператори відкрили спеціальні web-сторінки, свого роду дошки оголошень. Люди могли залишати на них свої повідомлення, навіть у відсутність мобільного зв'язку. Прочитати це повідомлення могла будь-яка людина, яка вводила в форму номер телефону того, хто його написав. Google запустив програму «Пошук людей», за допомогою якої користувачі можуть або вводити інформацію щодо когось, або шукати інформацію про когось, хто міг постраждати від цунамі. Крім того, один з найбільших операторів зв'язку NTT Docomo пропонує послугу (в тому числі – через спеціальний веб-портал, оформлений підкреслено з мінімальною кількістю об'єктів, що можуть заважати якнайшвидшому завантаженню на мобільний телефон), за допомогою якої люди могли зареєструвати до 10 адрес (номерів телефонів) людей із запитом щодо того чи в безпеці вони. Схожі за цільовим призначенням є сервіси KDDI Disaster Message Board, Softbank Message Board. У Японії існують плани евакуації і мешканці знають, хто і куди пересувається, знають адреси притулків, знають як до них добиратися і скільки у них є часу. Водночас в мережі Інтернет було запущено послугу Japan Shelter Map, яка фактично являла собою частину сервісу Google Map де були позначені місця, де люди могли відпочити, отримати допомогу та переночувати [101].

Таким чином, використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту дозволяє суттєво оптимізувати заходи щодо оповіщення громадян про небезпеку, удосконалити механізми порятунку та пошуку потерпілих від природного катаклізму чи техногенної катастрофи тощо.

За результатами проведеного аналізу механізмів попередження та інформування населення в умовах загрози або виникнення надзвичайної ситуації на прикладі природної та техногенної катастрофи в Японії Д. Дубов, М. Ожеван, А. Баровська сформулювали наступні висновки та рекомендації: система раннього сповіщення Японії виявилась в цілому ефективною та виконала більшість із поставлених задач – мінімізувала втрати серед населення та не допустила всеохоплюючої паніки; значною мірою така ефективність була обумовлена як технологічною готовністю японського уряду та спеціальних служб (максимальна автоматизація процесу сповіщення та його всеохопність), так і підготовленістю самого населення (внаслідок послідовно впроваджуваної системи навчань на всіх рівнях); значну роль у даній системі зіграв високий рівень інформатизації країни і, зокрема, мобільний зв'язок та доступність мережі Інтернет, що дозволило забезпечити попередньою інформацією про стихійне лихо кожного громадянина країни; на нормативно-правовому рівні використання телекомунікаційних мереж приватних компаній в умовах надзвичайних ситуацій в Україні все ще неврегульовано в повному обсязі (на даний момент така взаємодія більшою мірою залежить від доброї волі операторів, а процедур безпосередньої взаємодії в більшості своїй не існує); вбачається доцільним дослідити закордонний досвід (в першу чергу тих країн, що часто зазнають техногенних чи природних катастроф) щодо принципів взаємодії держави та приватних операторів телекомунікацій (включно із системою покарань для них у разі порушення) в умовах надзвичайних ситуацій [101].

Таким чином, досвід Японської Держави щодо організації загальної системи оповіщення населення про настання надзвичайної ситуації, а також

позитивний досвід координації сил та засобів цивільного захисту із використанням новітніх інформаційних технологій заслуговує на увагу та запозичення з метою імплементації в національне законодавство та практику цивільного захисту.

В Україні наразі чинним є Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, затверджене постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733 [250].

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 [250].

Таким чином, в Україні, як і в Японській Державі оператори електронних комунікацій, аудіальні та аудіовізуальні медіа, а також підприємства, установи, організації незалежно від форми власності і господарювання повинні приймати участь в оповіщені органів виконавчої влади, органів місцевого самоврядування, підприємств, установ, організацій, органів управління і сил цивільного захисту та населення про загрозу виникнення або виникнення надзвичайних ситуацій. Головним питанням залишається забезпечення координації сил та засобів щодо здійснення такого

оповіщення, залучення до його організації всіх суб'єктів господарювання, які надають телекомунікаційні послуги.

На увагу заслуговує також досвід Японської Держави щодо публічного управління у сфері пожежної безпеки.

Так, С. Говорун зазначає, що стійка тенденція до зниження пожеж та кількості загиблих на них, є наслідком проведеної реформи державного управління у сфері пожежної безпеки Японії, а також сталістю, внутрішньою несуперечливістю та узгодженістю законодавчої бази, якою керуються відповідні державні служби, а також приватні підприємства Японії [76, с. 29].

Таким чином, у сфері забезпечення пожежної безпеки також спостерігається притаманна Японії висока якість законодавства, зумовлена високим рівнем загальної правової культури в Японській Державі та високим рівнем правосвідомості громадян, які неухильно дотримуються правових традицій та звичаїв.

Крім того, С. Говорун підкреслює, що державне управління у сфері забезпечення пожежної безпеки Японії, регулюються виключно спеціальними законами, у яких чітко регламентовані суб'єкти, об'єкти державного управління у сфері забезпечення пожежної безпеки, їх права і обов'язки, на законодавчому рівні затверджується категоріальний апарат, котрим керуються у даній сфері [76, с. 48].

Так, 7 березня 1948 року у Японії набув чинності «Закон про організацію боротьби з пожежами і стихійними лихами», згідно із яким управління місцевими органами влади у сфері пожеж та ліквідації наслідків стихійних лих засновано на принципі запобігання пожежам та ліквідації наслідків пожеж і надзвичайних ситуацій. Згідно зі статтею 2 цього Закону, у тому ж 1948 році було створено Агенцію із боротьби з пожежами та ліквідації наслідків стихійних лих – Fire and Disaster Management Agency (FDMA), як зовнішню структуру Міністерства внутрішніх справ та зв'язку Японії відповідно до пункту 2 статті 3 Закону «Про організацію національного уряду» (National Government Organization Act (Act №. 120 of 10 July 1948) [76, с. 35].

У цьому ж році було прийнято Закон (Акт) про пожежну службу (Act №. 186, July 24, 1948), метою якого є підтримання миру та порядку, а також сприяння суспільному добробуту шляхом запобігання, захисту від пожеж та контролю за ними, захисту життя людей, осіб та майна від пожеж та мінімізації збитків, спричинених пожежами, землетрусами чи іншими лихами [358].

В даному випадку слід підкреслити сталість (стабільність) національного законодавства Японії та стабільність функціонування органів публічної адміністрації, які реалізують державну політику Японської Держави у сфері забезпечення пожежної безпеки. Цей досвід вартий запозичення Україною, адже постійні реформи центральних органів виконавчої влади, включаючи органи публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, не сприяють їх ефективній роботі, що включає формування традицій, злагодженості колективів, внутрішньої субкультури тощо.

Обов'язками FDMA є захист життя, здоров'я та майна громадян шляхом створення та впровадження у життя суспільства системи протипожежної безпеки, а також ведення справ, пов'язаних з протипожежною діяльністю, в тому числі для вирішення широкого кола питань. Із метою виконання вказаних обов'язків FDMA відповідає за наступні питання: питання, що стосуються створення та впровадження системи протипожежної безпеки на загальнодержавному рівні та складання правил пожежної безпеки; питання, пов'язані з класифікацією міських територій з точки зору протипожежного захисту (крім тих, що знаходяться під юрисдикцією префектурного уряду); питання, пов'язані зі здійснення заходів контролю, протипожежним управлінням та іншими протипожежними інституціями; питання, що стосуються розслідування причин пожеж та розслідування причин витоку небезпечних матеріалів або будь-якої іншої аварії; питання, що стосуються розробки та введення в дію стандартів освіти та підготовки працівників протипожежної служби (тобто, пожежних та іншого персоналу) та волонтерів пожежних корпусів; питання, що стосуються навчання та підготовки

працівників протипожежної служби та волонтерів пожежних корпусів; веде статистику діяльності пожежної охорони та збирає інформацію щодо стану протипожежного захисту; питання, що стосуються сертифікації та експертизи обладнання, машин, інструментів та матеріалів, які будуть використовуватися для цілей протипожежного захисту; питання, пов'язані з випробуваннями та дослідженнями щодо протипожежного захисту; питання, що стосуються керівництва та надання субсидій для посилення та розширення оснащення засобами протипожежної безпеки; питання щодо поширення та оприлюднення заходів із протипожежного захисту (паблік рілейшнз); питання, що стосуються способу оцінки небезпечних матеріалів та забезпечення їх безпеки, тощо [76, с. 36].

FDMA, також, опікується питаннями, які стосуються стандартів діяльності служби швидкої медичної допомоги, взаємодії між національними та місцевими органами влади та між органами місцевого самоврядування стосовно вирішення справ місцевого самоврядування, пов'язаними із плануванням робіт та проведенням інспекційних перевірок, а також іншими питаннями, пов'язаними із забезпеченням безпеки комерційних об'єктів нафтохімічної промисловості. До відома FDMA входять питання, що стосуються міжнародної допомоги в надзвичайних ситуаціях, міжнародного співробітництва; питання, пов'язані з евакуацією мешканців та питання, що стосуються взаємодії та координації між національним та місцевими урядами, а також між органами місцевого самоврядування [76, с. 36].

Таким чином, коло питань забезпечення пожежної безпеки в Японський Державі, за які відповідає FDMA, є достатньо широким, що вимагає детального адміністративно-правового регулювання на рівні відомчої нормотворчості, а також використання інноваційних інформаційних технологій для забезпечення обробки значних масивів інформації, надання відповідних електронних (цифрових) адміністративних послуг та постійного зв'язку з іншими органами публічної адміністрації, протипожежними службами та волонтерами пожежних корпусів.

FDMA є центральним державним органом, який координує діяльність усіх інших міністерств, відомств, префектур, муніципалітетів щодо запобігання, ліквідації та відновлення об'єктів інфраструктури в разі настання надзвичайних ситуацій, а також щодо здійснення профілактики та гасіння пожеж. Названа урядова організація активно працює у всіх префектурах, муніципалітетах районах, містах і селищах Японії, починаючи від впровадження пожежно-аварійної діяльності, до контролю над поводження із небезпечними матеріалами, а також проведення інспекційних перевірок дотримання правил і норм пожежної безпеки [76, с. 36-37].

С. Говорун зазначає, що організаційна структура державного управління Японії у сфері забезпечення пожежної безпеки і подолання стихійних лих та їх наслідків має три рівні. Найвищий – національний рівень забезпечення пожежної безпеки (згідно із Законом «Про організацію протипожежної охорони»), який встановлює, що FDMA проводить дослідження, формулює плани розвитку і діяльності системи організації протипожежної служби з метою посилення спроможності муніципалітетів щодо їх протипожежного захисту. Для досягнення цієї мети FDMA надає муніципалітетам поради, керівні вказівки та рекомендації щодо організації та здійснення заходів згаданою службою. Однак FDMA не має повноважень повністю контролювати діяльність муніципалітетів із даного напрямку [76, с. 37].

Найбільш повно інформація про діяльність FDMA (Fire and Disaster Management Agency) представлена на його офіційному веб-сайті – https://www.fdma.go.jp/en/, включаючи основні цілі агентства (Місія Агентства з боротьби з пожежами та стихійними лихами), стандарти, організацію, юрисдикцію та законодавчу основу його діяльності (Закон про пожежну службу та інші відомчі нормативні акти), інформацію про систему перевірки протипожежного обладнання та інструментів, звіти про об'єкти з небезпечними матеріалами тощо [358].

Так, до цілей (місій) Агентства з боротьби з пожежами та стихійними лихами віднесено: готовність до великомасштабних катастроф, таких як землетрус у Нанкайському жолобі та землетрус у внутрішній частині Токіо; місія рятувати життя, які можна врятувати; запобігання пожежам і промисловим катастрофам; поліпшення боротьби зі стихійними лихами в громадах із центральною роллю Добровольчого пожежного корпусу; захист людей від тероризму та збройних нападів; розвиток людських ресурсів та використання нових технологій.

На другому рівні системи забезпечення пожежної безпеки знаходяться префектури Японії. Префектури не беруть безпосередньої участі в ліквідації надзвичайних ситуації, але мають консультативну й координувальну владу над муніципалітетами, які, у свою чергу, стоять на третьому – нижньому рівні системи державного управління у сфері пожежної безпеки Японії. Під юрисдикцію префектур підпадає виконання таких обов'язків: зв'язок та координація між міськими пожежними службами; надання порад і рекомендацій стосовно устрою та діяльності пожежних служб міста; визначення напрямку щодо здійснення заходів із попередження стихійних лих та здійснення запитів про надання допомоги під час надзвичайних ситуацій; навчання та підготовка працівників пожежної служби та волонтерів у префектурних пожежних Академіях; розроблення та прийняття префектурних планів з попередження стихійних лих та реалізації всебічних контрзаходів протидії наслідкам стихійних лих [76, с. 37].

Таким чином, на рівні префектур органами публічної адміністрації Японської Держави також активно використовуються інформаційні технології з метою організації зв'язку та здійснення координації між міськими пожежними службами, розробки префектурних планів з попередження стихійних лих, а також накопичення та обробки інформації про надзвичайні події та їх наслідки, наявні сили та засоби цивільного захисту тощо.

Слід відзначити, що в Україні План реагування на надзвичайні ситуації державного рівня затверджений Постановою Кабінету Міністрів України від 14 березня 2018 р. № 223 [244].

Зазначений План реагування на надзвичайні ситуації державного рівня розроблено для впорядкування та координації дій органів державної влади України, органів місцевого самоврядування, органів управління та сил цивільного захисту, суб'єктів господарювання, спрямованих на ліквідацію наслідків та надання допомоги постраждалим, у разі загрози виникнення або виникнення надзвичайної ситуації [244].

І вже на основі вказаного плану розробляються конкретизовані плани ліквідації надзвичайних ситуацій на місцевому, регіональному рівні.

Третій рівень, який однак є найбільш поширеним рівнем системи забезпечення пожежної безпеки та ліквідації наслідків катастроф, що лежить в основі «піраміди» протипожежного захисту Японії – це муніципальний рівень. Згідно зі ст. 10 Закону «Про організацію протипожежної охорони» «створення, місцезнаходження та назви штабів пожежної охорони та пожежних станцій, а також окреслення районів юрисдикції пожежних станцій визначаються муніципальним розпорядженням. Організація штабу пожежної охорони визначається муніципальними правилами, тоді як організаційну структуру і чисельний склад пожежної станцій визначає її начальник із затвердженням мером відповідного муніципалітету» [76, с. 38].

Муніципалітети Японії зобов'язані повністю опікуватися створенням і функціонуванням пожежної служби у межах своєї юрисдикції. Вони фактично впроваджують та реалізують діяльність служб протипожежного захисту, такі як пожежні та рятувальні служби, а також служби швидкої допомоги. У Японії вважається, що більш ефективно та раціонально слід провадити роботу в даному напрямку спільно з іншими муніципалітетами. Такий підхід прийнятий із огляду на фінансову складову справи. Деякі муніципалітети роблять це шляхом створення «муніципальних корпорацій» або «асоціацій районів». Організації із протипожежного захисту складаються із пожежних

департаментів, пожежних станцій та волонтерських пожежних корпусів. Муніципалітети зобов'язані організувати деякі із названих протипожежних закладів або їх всі. Пожежні департаменти та пожежні станції укомплектовуються професійними пожежниками, а пожежний корпус складається із пожежних-волонтерів, які мають власну трудову діяльність або зайнятті на іншій найманій роботі. Пожежний корпус (пожежні волонтери) є незалежним у своїй організаційній діяльності від пожежних департаментів та пожежних станцій, та між ними немає ніяких вертикальних субординаційних відношень. Однак у випадках, коли у разі пожежі або іншої надзвичайної ситуації залучається пожежний корпус, його посадові особи та інші члени повинні дотримуватися розпоряджень начальника пожежного департаменту або пожежної станції. У такий спосіб реалізується принцип єдиноначальності при проведені операцій із гасіння пожеж та ліквідації наслідків стихійних лих та інших катастроф [76, с. 38].

Таким чином, саме на рівні муніципалітетів, тобто органів місцевого самоврядування в Японській Державі вирішуються ключові питання щодо створення і функціонування служб протипожежного захисту, що включають пожежні та рятувальні служби, а також служби швидкої допомоги.

На увагу заслуговує досвід Китайської Народної Республіки щодо організації цивільного захисту із залученням народного ополчення. Так, В. Гастинщиков, аналізуючи систему народної самооборони Китаю, зазначає, що під час масштабних військових навчань, що відбуваються в китайській армії, на підрозділи Військ народного ополчення покладається дедалі більше обов'язків та завдань. Система народної самооборони Китаю, яка налічує до восьми мільйонів осіб, значно перевершує за чисельністю збройні сили. Вона активно використовує демобілізованих ветеранів і цивільні організації, які підписали угоди про співпрацю з армією. Під час надзвичайних ситуацій цей персонал може бути розгорнуто для доповнення місцевих сил НВАК (Національної визвольної армії Китаю). Наприклад, на початку липня понад 400 ополченців допомагали особовому складу НВАК ліквідовувати наслідки

руйнівній повені в Чунціні. Ополченці займалися пошуково-рятувальними роботами, розчищали дороги, також проводили евакуацію мирних жителів із небезпечної зони. Також цивільні підприємства часто співпрацюють з армією, наприклад, одна з філій китайської залізниці China Railway Group надала своє обладнання та потужності для проведення екстреного ремонту під час навчань [74].

Раніше Китай зробив значний крок у розвитку потенціалу ополчення та його інтеграції з НВАК: він створив Департамент мобілізації національної оборони, який, серед іншого, інспектує різні регіони країни, оцінюючи їхні можливості щодо допомоги армії та розробляє методи покращення військової інтеграції під час бойових дій або національної кризи [74].

На окрему увагу заслуговує також досвід КНР щодо правового регулювання використання інноваційних інформаційних технологій, зокрема, технології штучного інтелекту.

Так, у Верховному суді Китаю заявили, що підтримують законне застосування штучного інтелекту та захищають інновації відповідно до законодавства. Також було заявлено, що Верховний суд Китаю цього року посилить захист штучного інтелекту та інтелектуальної власності, оскільки країна прагне розвивати нові галузі [61].

Частина звіту про роботу суду була присвячена шляхам стимулювання таких інновацій та стримування зловживань у сфері штучного інтелекту, а також інших технологій. Стрімке зростання китайського стартапу DeepSeek у сфері штучного інтелекту продемонструвало, наскільки швидко можуть змінюватися перспективи високотехнологічного сектору Китаю, але водночас викликало занепокоєння ризиками, пов’язаними з патентними спорами, порушенням конфіденційності та наклепом [61].

Таким чином, КНР наразі є одним із лідерів у сфері впровадження технології штучного інтелекту, включаючи його використання у сфері забезпечення безпеки життєдіяльності.

На увагу заслуговує також досвід організації та правового забезпечення

функціонування системи цивільного захисту та механізму забезпечення безпеки життєдіяльності в цілому в Державі Ізраїль, адже Ізраїль як і Україна знаходиться в стадії активних бойових дій (обумовлених зовнішньою воєнної агресією), що створює подвійне навантаження на загальнодержавну систему цивільного захисту обох країн.

Нормативне регулювання функціонування системи цивільної оборони Ізраїлю здійснюється відповідно до Закону про цивільну оборону від 1951 р. [361] та низки підзаконних актів. Вони регламентують деякі питання захисту та укриття цивільного населення у сховищах, побудованих в усіх житлових будинках, на промислових об'єктах і у громадських місцях; контролюють залучення приватної власності до забезпечення заходів цивільної оборони в умовах ліквідації наслідків надзвичайних ситуацій (стихійних лих і аварій на підприємствах); визначають спроможності та рівень готовності до захисту цивільного населення, а також встановлюють правила поводження з небезпечними речовинами [308, с. 321].

Показовою в даному випадку є стабільність законодавства Держави Ізраїль у сфері правового регулювання організації цивільної оборони, адже часта зміна законів, які регулюють питання забезпечення безпеки життєдіяльності, не сприяє формуванню правових традицій та звичаїв, правосвідомості та правової культури у вказаній сфері суспільних відносин. Такий зарубіжний досвід адміністративно-правового регулювання суспільних відносин у сфері забезпечення безпеки життєдіяльності та цивільного захисту заслуговує на увагу та впровадження в національну юридичну практику.

Загальне керівництво системою цивільної оборони Держави Ізраїль здійснює Командування внутрішнього фронту (тилу) Ізраїлю, створене в лютому 1992 р. Командування тилу є четвертим командуванням ЦАХАЛ, що включає HAGMAR (регіональна оборона) та HAGA (цивільна оборона). Командування внутрішнього фронту (тилу) Ізраїлю нині відповідає за питання цивільної оборони і проведення пошуково-рятувальних операцій в цивільному секторі. Місія Командування внутрішнього фронту (тилу) полягає у посиленні

національної стійкості та рятуванні життів цивільного населення в умовах кризових ситуацій, проведенні заходів підготовки до дій в докризовий період, у фазі реагування на кризу та під час пошуково-рятувальних операцій у разі атаки на тил, а також під час планування та безпосереднього відновлення цивільного простору в посткризовій фазі. Також Командування тилу інформує цивільне населення щодо правил поведінки в умовах загрози і публікує регулярні інструкції з цивільної оборони, особливо під час надзвичайних ситуацій природного і техногенного характеру. Для звернення громадян у разі небезпеки функціонує центр екстреної допомоги за номером 104 [308, с. 322].

Таким чином, в Державі Ізраїль, враховуючи триваючий роками військових конфлікт із сусідніми арабськими державами, належний рівень організації та правового забезпечення цивільної оборони є ключовим чинником виживання держави та суспільства. Триваюча війна обумовлює те, що орган публічної адміністрації, який реалізує державну політику у сфері цивільного захисту в Державі Ізраїль, є одним із підрозділів військового керівництва держави і має відповідну назву – Командування внутрішнього фронту (тилу).

На Командування внутрішнього фронту (тилу) покладено реалізацію таких завдань у сфері цивільної оборони: розроблення нормативних документів з питань цивільної оборони; розроблення планів цивільної оборони для всієї країни та окремих територіальних одиниць; управління діяльністю національної служби екстреної медичної допомоги, катастроф, швидкої допомоги та банку крові Ізраїлю (Magen David Adom), навчання та тренування персоналу цієї служби, а також управління пожежними і рятувальними службами та іншими допоміжними організаціями щодо виконання їхніх обов’язків у сфері цивільної оборони; регулювання діяльності посадових осіб в умовах реалізації заходів цивільної оборони щодо захисту цивільного населення в умовах надзвичайних ситуацій природного і техногенного характеру та ракетно-бомбових атак; керівництво органами місцевого самоврядування щодо виконання покладених на них обов’язків з питань

цивільної оборони; координація діяльності міністерств, приватних підприємств, національної інфраструктури з питань цивільної оборони; міжвідомча та міжсекторальна взаємодія у сфері цивільної оборони; радіаційний та хімічний захист населення і територій, проведення деконтамінації та нормування діяльності, пов'язаної з використанням небезпечних речовин; інформування та оповіщення цивільного населення про небезпеки та правила безпекової поведінки в умовах загроз; накопичення та зберігання оперативних запасів засобів індивідуального захисту для цивільного населення, а також їх розподіл; проведення пошуково-рятувальних робіт [308, с. 323].

Таким чином, Командування внутрішнього фронту (тилу) є ключовим органом публічної адміністрації, який реалізує політику Держави Ізраїль у сфері цивільного захисту, і, як показує практика, суттєву роль в організації діяльності Командування внутрішнього фронту (тилу) відіграють саме інформаційні технології, які дозволяють здійснювати координацію діяльності інших органів публічної адміністрації, медичних, пожежних і рятувальних служб, а також допоміжних організацій з метою оперативної ліквідації надзвичайних ситуацій та їх наслідків.

Крім того, А. Терент'єва зазначає, що у вересні 2007 р. в Державі Ізраїль утворене Національне агентство з надзвичайних ситуацій, яке відповідає за координацію військових і цивільних дій під час надзвичайного стану, війни або стихійного лиха. Зоною відповідальності агентства визначено координацію спільних дій та забезпечення міжвідомчої взаємодії під час реагування на кризи та надзвичайні ситуації, а також організацію і супровід навчань з питань цивільної оборони та захисту цивільного населення [308, с. 323-324].

Таким чином, в Державі Ізраїль особлива увага приділяється питанням оповіщення населення про небезпеки та правила безпекової поведінки в умовах загроз, а також організації навчань з питань цивільної оборони та захисту цивільного населення. Провідну роль в організації цивільної оборони

відіграють сучасні інформаційні технології, зокрема, використання автоматизованих інформаційних систем, мобільних застосунків тощо.

Ізраїльська пожежно-рятувальна служба є національною пожежно-рятувальною організацією, яка також здійснює заходи з порятунку в умовах терористичних атак, автомобільних аварій та розливів небезпечних речовин разом із національною службою швидкої допомоги. Служба бере участь у громадських просвітницьких та інформаційних кампаніях. Після лісової пожежі на горі Кармель у 2010 р., внаслідок якої загинуло багато людей, уряд створив Ізраїльське пожежно-рятувальне управління та організував пожежно-рятувальну службу на національному рівні, як і поліцію. Наразі ізраїльська пожежно-рятувальна служба складається із близько 2500 професійних пожежників, а також ще з 200-400 добровольців-пожежників, які проходять відповідний вишкіл. Підготовка пожежників в Ізраїлі проводиться у Національній пожежно-рятувальній школі, починаючи з 1979 р. [308, с. 325].

Крім того, у складі служби функціонує 11 підрозділів для проведення заходів хімічного, радіаційного та біологічного захисту, що мають відповідне оснащення. Всі станції забезпечують пошуково-рятувальні роботи і пожежогасіння та оснащені найновішим обладнанням [308, с. 326-327].

Отже, позитивним є досвід Держави Ізраїль щодо залучення добровольців-пожежників для ліквідації надзвичайних ситуацій, причому їх підготовці приділяється особлива увага.

За результатами аналізу досвіду Держави Ізраїль щодо управління безпекою цивільного населення в умовах кризових ситуацій А. Терент’єва стверджує, що ізраїльська національна безпекова доктрина, випробувана всією історію державотворення, підтвердила ефективність свого існування під час захисту цивільного населення в умовах воєнного протистояння, що постійно триває. Причому, саме на місцеву владу покладено завдання щодо створення оборонної інфраструктури та розроблення порядків розгортання сил і засобів для захисту цивільного населення в умовах надзвичайних ситуацій природного і техногенного характеру та бойових дій. Тобто до сфери

компетенцій органів місцевої влади Ізраїлю належить створення територіальної підсистеми оборони та захисту тилу, підтримка обороноздатності, захист цивільного населення та об'єктів критичної інфраструктури [308, с. 329-330].

Також А. Терент'єва зазначає, що в Державі Ізраїль вибрано воєнно-орієнтований підхід до управління в умовах кризових ситуацій. Подібний підхід у реаліях країни забезпечує можливість застосування моделі внутрішнього фронту (тилу) в умовах надзвичайних ситуацій природного і техногенного характеру та бойових дій, що підтверджується позитивним досвідом функціонування системи «Iron Dome» [308, с. 329-330].

Таким чином, враховуючи багаторічний досвід Держави Ізраїль у сфері організації та правового забезпечення функціонування системи цивільної оборони в умовах воєнного стану, проаналізований вище воєнно-орієнтований підхід до управління в умовах кризових ситуацій заслуговує на увагу та імплементацію в національне законодавство та юридичну практику.

Висновки до розділу 3

1. Проведене дослідження досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі дає підстави сформулювати висновок про те, що в Механізмі цивільного захисту Європейського Союзу використовуються такі інформаційні технології як інформаційні платформи, бази даних, засоби оперативного зв'язку та координації тощо. Використання вказаних інформаційних технологій має належну правову регламентацію на рівні рішень Європейського парламенту та Європейської Ради.

До правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід віднести GDPR – Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне

переміщення таких даних, а також Європейський закон (Регламент) про штучний інтелект (Artificial Intelligence Act, AI Act).

Важливими документами щодо регулювання розвитку цифровізації в Європейському Союзі також є Європейська структура сумісності (EIF), яка надає загальний набір стандартів для забезпечення легкого доступу до державних послуг і спільного використання в усьому ЄС, а також Регламент eIDAS, що визначає правила електронної ідентифікації та довірчих послуг у всьому ЄС.

Враховуючи необхідність завершення процесів євроінтеграції, національним органам публічної адміністрації, зокрема Міністерству цифрової трансформації України, необхідно активізувати участь національних державних та приватних інституцій у розвитку Єдиного цифрового ринку ЄС, залучати інвестиції для розвитку національного цифрового ринку, включаючи фінансування заходів із забезпечення кібербезпеки. Крім того, одним із завдань є завершення процедур адаптації національного законодавства в частині правового регулювання використання інформаційних технологій та забезпечення безпеки життєдіяльності до права ЄС.

2. Проведене дослідження особливостей адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в США дає підстави сформулювати висновок про можливість та доцільність запозичення позитивного досвіду органів публічної адміністрації США в частині адміністративно-правової регламентації діяльності у сфері цивільного захисту населення і територій від надзвичайних ситуацій. Зокрема, до позитивного досвіду слід віднести розробку та реалізацію FEMA Федерального плану, який є головним актом у процесі реагування на надзвичайну ситуацію та ліквідацію її наслідків. Також позитивним є досвід побудови структури та організації діяльності Федерального агентства з управління надзвичайними ситуаціями (FEMA), зокрема його функції щодо адміністрування та координації діяльності інших органів публічної адміністрації у вказаній сфері суспільних відносин.

Варто запозичити, зокрема, структуру та зміст офіційного сайту FEMA, який містить детальну інформацію як для суб'єктів владних повноважень, так і для громадян щодо організації цивільного захисту населення та територій США від надзвичайних ситуацій.

На увагу заслуговує також досвід FEMA у сфері координації діяльності органів публічної адміністрації щодо своєчасного реагування на надзвичайні ситуації та оперативної ліквідації їх негативних наслідків, а також акумулювання інформації про надзвичайні ситуації, що забезпечується засобами комунікації з використанням новітніх інноваційних інформаційних технологій (швидкісного оптоволоконного зв'язку, захищеного серверного обладнання, хмарних технологій, можливостей соціальних мереж та месенджерів, технології штучного інтелекту тощо).

Позитивний досвід США щодо розроби та реалізації федерального плану реагування на надзвичайні ситуації імплементовано в національне законодавство на рівні постанови Кабінету Міністрів України від 14 березня 2018 р. № 223 «Про затвердження Плану реагування на надзвичайні ситуації державного рівня», що дозволяє національним органам публічної адміністрації оперативно реагувати на надзвичайні ситуації.

3. Проведене дослідження адміністративно-правових засад забезпечення безпеки життєдіяльності та цивільного захисту в Японській Державі в умовах цифровізації дозволяє сформулювати висновок про доцільність запозичення трирівневної системи публічного управління ліквідацією надзвичайних ситуацій та їх наслідків в Японській Державі, в якій ключову роль відіграє рівень муніципалітетів, тобто організація сил та засобів цивільного захисту на рівні органів місцевого самоврядування, що дозволяє максимально оперативно реагувати на початок надзвичайної ситуації, а також проводити систематичні навчання та тренінги із населенням у сфері цивільного захисту.

Також слід підкреслити сталість національного законодавства Японії та стабільність функціонування органів публічної адміністрації, які реалізують державну політику Японської Держави у сфері забезпечення пожежної

безпеки. Цей досвід вартий запозичення Україною, адже постійні реформи центральних органів виконавчої влади, включаючи органи публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, не сприяють їх ефективній роботі, що включає формування традицій, злагодженості та згуртованості колективів, внутрішньої субкультури тощо.

Позитивним є досвід Японської Держави щодо створення «муніципальних корпорацій» або «асоціацій районів» з метою консолідації фінансових та організаційних ресурсів для ліквідації надзвичайних ситуацій. Також позитивним є досвід щодо функціонування волонтерських пожежних корпусів, які складаються із пожежних-волонтерів, які мають власну трудову діяльність або зайнятті на іншій найманій роботі (однак у разі пожежі або іншої надзвичайної посадові особи та інші члени волонтерських пожежних корпусів повинні дотримуватися розпоряджень начальника пожежного департаменту або пожежної станції).

На увагу заслуговує також ізраїльська національна безпекова доктрина, ефективність існування якої підтверджена під час захисту цивільного населення в умовах воєнного протистояння, що постійно триває. Для України, яка знаходиться у схожій ситуації, актуальною є ізраїльська модель поєднання сил та засобів органів військового управління та цивільних органів публічної адміністрації в організації ліквідації надзвичайних ситуацій та їх наслідків, включаючи використання сучасних інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а саме новітніх систем оповіщення цивільного населення про загрозу ракетних обстрілів.

Позитивним також є досвід Держави Ізраїль щодо залучення добровольців-пожежників для ліквідації надзвичайних ситуацій.

Підсумовуючи слід зазначити, що воєнно-орієнтований підхід до управління в умовах кризових ситуацій в Ізраїлі заслуговує на більш детальне дослідження та імплементацію в національне законодавство та юридичну практику.

РОЗДІЛ 4
АКТУАЛЬНІ НАПРЯМИ УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ В КОНТЕКСТІ ЦИФРОВІЗАЦІЇ

4.1 Адміністративно-правові засади цифровізації системи публічного управління в Україні

Забезпечення безпеки життєдіяльності в сучасному світі є одним із найбільш актуальних питань цивілізації. Технологічний прогрес, розвиток інформаційних технологій призвели до формування кардинально нової системи суспільних відносин, в якій цифрові товари та послуги вийшли фактично на один рівень з енергоресурсами та цінними металами, а подекуди і перевершили їх за собівартістю. Крім того, цифровізація відбулась і в гуманітарній сфері, змінивши підходи до освіти та наукової діяльності, а також у сфері медицини та в інших сферах суспільного життя.

У сфері публічного управління впровадження інформаційних технологій дозволило значно оптимізувати, удосконалити процеси адміністрування суспільних відносин, надання адміністративних послуг, в значні мірі перейти на електронний документообіг, що в свою чергу дозволило суттєво економити фінансові та матеріально-технічні ресурси.

Враховуючи вищезазначене, сучасне суспільство по праву називають інформаційним, адже інформація стала по суті основою економіки, універсальним засобом виробництва, а інформаційні технології дозволили вийти на новий рівень розвитку цивілізації. Наприклад, за даними Державної служби статистики України, у 2017 році продукція сектору інформаційних технологій становила більше ніж 3 відсотки валового внутрішнього продукту, а сукупний дохід галузі – більше ніж 3,5 млрд. доларів США, що співставно з обсягами продукції високотехнологічного сектору [285].

У зв’язку із вищевикладеним, науковці приділяють значну увагу визначенню поняття інформаційного суспільства.

Так, В.П. Степаненко в електронній Енциклопедії сучасної України надає наступне визначення інформаційного суспільства: це соціологічна концепція постіндустріального суспільства; нова історична фаза розвитку суспільства, в якому виробництво, використання та споживання інформації стає визначальним способом діяльності в усіх сферах суспільного буття (економіці, політиці та культурі). Особливістю цього типу суспільства є вирішальна роль інформаційно-комунікаційних технологій (ІКТ), виробництво інформації та знання [303].

Отже, саме інформаційні технології є ключовою категорією інформаційного суспільства, а рівень їх розвитку визначає ступінь зрілості, сформованості та конкурентоздатності сучасного суспільства.

В. Бебик зазначає, що під інформаційним суспільством потрібно розуміти сучасне суспільство з високим рівнем розвитку інформаційної культури (створення, переробки та використання інформації), яке характеризується: здатністю якісно продукувати всю необхідну для життєдіяльності суспільства інформацію; наявністю розвиненої інформаційної інфраструктури суспільства; високим рівнем доступності для всіх членів суспільства необхідної інформації; великою часткою працездатного населення, що працює в інформаційному секторі економіки. Крім того, на його думку, інформаційне суспільство характеризується визнанням інформації одним з найважливіших суспільних ресурсів, а інформаційний сектор економіки (виробництво, зберігання, обробка, передача і споживання інформації) є одним з найважливіших видів суспільної діяльності, який створює інформаційно-комунікаційну базу для формування глобального інформаційного суспільства та розвитку науково-технічного, соціально-економічного й освітньо-культурного прогресу [21, с. 41].

Таким чином, науковці в основному відзначають позитивні тенденції формування та розвитку інформаційного суспільства.

Проте, окрім позитивних аспектів, цифровізація суспільних відносин зумовила появу значної кількості негативних факторів, які впливають на людину та суспільство в цілому.

По-перше, це спрощення доступу до персональних даних фізичних осіб в інформаційному суспільстві, адже люди самі викладають данні про себе в Інтернет, зокрема, соціальні мережі, пересилають скановані копії документів тощо. Такий спрощений доступ створює умови для зростання кількості випадків використання персональних даних з протиправною метою (шахрайства, вимагання тощо).

По-друге, це нові загрози інформаційній безпеці у сфері публічного управління, що включають хакерські атаки на органи публічної адміністрації, тобто несанкціонований доступ до публічних інформаційних ресурсів, державних реєстрів з метою викрадення, спотворення або знищення відповідної інформації.

По-третє, це підвищення ризику катастроф техногенного характеру через можливі перебої в роботі автоматизованих систем, зумовлені несанкціонованим доступом до них або помилками в роботі програмного забезпечення.

По-четверте, це використання інформаційних технологій у військових цілях, зокрема для ведення інформаційної війни, або для удосконалення зразків сучасної летальної зброї (наприклад, виробництва роботизованих систем, безпілотних літальних апаратів зі штучним інтелектом).

По-п’яте, це загрози, які несе із собою неконтрольований розвиток технології штучного інтелекту, адже штучний інтелект діє за заданими алгоритмами і у випадку виникнення надзвичайної ситуації може заблокувати можливість виправити ситуацію з боку людини. Як приклад, це безпілотні автомобілі, які у випадку аварійної ситуації можуть не врахувати всі негативні фактори (які здатна виявити та врахувати людина), що призведе до загибелі або травмування пасажирів чи пішоходів. Використання технології штучного інтелекту у військових розробках може потенційно призвести до втрати

контролю над автоматизованою військовою технікою, яка буде продовжувати знищувати запрограмовані об’єкти навіть після припинення бойових дій людьми.

По-шосте, це поширення негативного, протиправного цифрового контенту – культу насильства та жорстокості, дитячої порнографії, пропаганди тероризму та екстремізму тощо.

По-сьоме, це використання інформаційних технологій для вчинення «класичних» злочинів: вимагання, шахрайства, хуліганства, погрози вбивством, психологічного залякування та цькування (булінгу), незаконного переслідування особи (включаючи сексуальні домагання), несанкціонованого стеження за особою, включаючи відеоспостереження, прослуховування її розмов та перегляд листування тощо.

Наведений перелік негативних факторів, які є наслідком цифровізації (розвитку інформаційного суспільства) та суттєво впливають на людину та суспільство в цілому, звичайно не є вичерпним, адже майже кожного року з’являються нові інформаційні технології, які потребують належного правового регулювання, якщо вони зачіпають права чи інтереси людини або можуть негативно вплинути на безпеку життєдіяльності людини чи суспільства в цілому.

Водночас інформаційні технології дозволяють значно удосконалити систему забезпечення безпеки життєдіяльності.

Так, до інформаційних технологій, які дозволяють оптимізувати механізми забезпечення безпеки життєдіяльності, слід віднести:

- автоматизовані системи: гасіння пожеж; зупинки виробництва; відключення електропостачання у випадку загрози настання надзвичайної ситуації або її безпосереднього початку; блокування транспортних шляхів, на яких склалася аварійно небезпечна ситуація або відбулась техногенна аварія; попередження про землетруси, цунамі тощо;

- мобільні застосунки, які дозволяють оперативно сповістити населення про загрозу чи початок надзвичайної ситуації, а також швидко мобілізувати

людські та матеріально-технічні ресурси для ліквідації надзвичайної ситуації та її наслідків;

- технологію «розумний дім», яка дозволяє людині дистанційно керувати електроприладами в будинку, отримувати в режимі онлайн результати відеоспостереження за станом домашнього господарства та оперативно реагувати на можливі загрози безпеці життєдіяльності;

- системи автоматизованого відеоспостереження за станом технологічних, виробничих потужностей підприємств, станом критичної інфраструктури, станом дорожнього руху тощо;

- автоматизовані датчики контролю рівня води, коливань ґрунту, хімічного складу речовин, викидів, біологічного та радіаційного контролю;

- технологію штучного інтелекту, яка акумулюючи інформацію з різних джерел здатна прогнозувати вірогідність настання надзвичайної ситуації природного чи техногенного характеру, а також оперативно реагувати на початок надзвичайної ситуації, автоматично застосовуючи засоби цивільного захисту (включаючи зупинку виробництва, електро- та водопостачання, активацію систем пожежогасіння та евакуації людей тощо).

З метою удосконалення механізмів забезпечення безпеки життєдіяльності вказані інформаційні технології поєднуються та комбінуються. Наприклад, автоматичні камери відеоспостереження на промислових об’єктах з’єднуються з комп’ютерною системою з елементами штучного інтелекту, а також з автоматизованими системами гасіння пожеж. У випадку потрапляння в «поле зору» об’єктива відеокамери зображення полум’я чи диму, комп’ютерна програма автоматично видає команду на активацію системи гасіння пожежі. Таким чином, на відміну від датчиків диму, які часто не спрацьовують через несправність, наведена комбінована система гасіння пожеж є більш надійною та ефективною, адже рідина для гасіння пожежі спрямовується чітко на місце її виявлення. Отже, ліцензування такої комбінованої системи та надання рекомендацій з боку органів публічної адміністрації щодо доцільності використання саме такого засобу забезпечення

безпеки життєдіяльності дозволить поширити відповідний позитивний досвід та підвищити рівень пожежної безпеки в цілому.

Таким чином, в умовах активного розвитку інформаційного суспільства адміністративно-правового регулювання потребує як використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, так і самі інформаційні технології, які становлять потенційну загрозу життю чи здоров'ю людини (можуть порушити нормальні умови життя і діяльності людей), нормальному функціонуванню та розвитку суспільства тощо.

Інформаційні технології (скорочено – ІТ) визначають як систему методів, процесів та способів використання обчислювальної техніки і систем зв'язку для створення, збору, передачі, пошуку, оброблення та поширення інформації з метою ефективної організації діяльності людей [213, с. 227].

У відповідності до Національної програми цифровізації, цифрова технологія – це сукупність систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій [265].

А створення засобу інформатизації – це сукупність правових, організаційних, адміністративних та інженерно-технічних заходів, яких вживає розпорядник (одержувач) бюджетних коштів для автоматизації одного чи декількох процесів, у тому числі для створення комплексної системи захисту інформації, включаючи визначення потреби та введення засобу інформатизації у промислову експлуатацію [265].

Таким чином, інформаційні технології – це всі існуючі та проектовані технічні та програмні засоби роботи з інформацією, включаючи використання комп'ютерів, серверів, телекомунікаційного обладнання, програмного забезпечення, Інтернет тощо.

Вказані технічні засоби справедливо називають цифровими інструментами або інструментами цифровізації, адже інформація в процесі її збору, передачі, обробки та зберігання переводиться у цифровий формат, що дозволяє значно оптимізувати, прискорити та автоматизувати вказані процеси.

Інформаційні технології настільки поширені в сучасному суспільстві, що останнє по праву називають інформаційним. Процеси цифровізації охопили фактично всі сфери суспільних відносин і без Інтернету, смартфону, планшету, комп'ютера чи ноутбука ми вже не уявляємо своє життя.

Цифрові (інформаційні) технології значно полегшують життя людини, проте і створюють нові проблеми, пов'язані із необхідністю захисту інформації, персональних даних, протидії поширенню шкідливого програмного забезпечення, дезінформації, спаму (інформаційного сміття) тощо. Суттєвою проблемою є використання інформаційних технологій із протиправною метою.

Вищевказаним обумовлюється необхідність правового врегулювання використання інформаційних технологій, тобто створення органами публічної адміністрації чітких правил гри в цифровому просторі, а також встановлення юридичної відповідальності за порушення вказаних правил.

Використання інформаційних технологій тісно пов'язано із забезпеченням безпеки життєдіяльності, адже, як вже було зазначено, інформаційні технології не тільки полегшують життя, але й створюють нові загрози життю та здоров'ю людей. Водночас вказані технології активно використовуються для автоматизації процесів забезпечення безпеки життєдіяльності, починаючи від систем охорони праці на підприємствах, в установах та організаціях, автоматизованих протипожежних систем, і закінчуючи використанням технології штучного інтелекту для прогнозування виникнення надзвичайних ситуацій та здійснення контролю показників різноманітних датчиків на об'єктах критичної інфраструктури та підвищеної небезпеки.

До правових засад цифровізації публічного управління та використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід віднести закони України:

- «Про інформацію» [261] – регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

- «Про захист інформації в інформаційно-комунікаційних системах» [258] – регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах;

- «Про обов’язковий примірник документів» [268] – визначає правові засади функціонування системи обов'язкового примірника документів та регулює інформаційні відносини, пов'язані з поповненням національного інформаційного фонду України;

- «Про електронні документи та електронний документообіг» [238] – встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів. Дія цього Закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів [238];

- «Про електронні комунікації» [239] – визначає правові та організаційні основи державної політики у сферах електронних комунікацій та радіочастотного спектра, а також права, обов’язки та відповідальність фізичних і юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами. Дія вказаного Закону поширюється на відносини у сферах електронних комунікацій та радіочастотного спектра щодо надання та отримання електронних комунікаційних послуг, постачання та доступу до електронних комунікаційних мереж, забезпечення конкуренції на ринках електронних комунікацій, а також щодо користування радіочастотним спектром, ресурсами нумерації та захисту прав користувачів послуг [239];

- «Про електронну ідентифікацію та електронні довірчі послуги» [240] – визначає правові та організаційні засади електронної ідентифікації та надання електронних довірчих послуг, права та обов'язки суб'єктів відносин у сферах електронної ідентифікації та електронних довірчих послуг, порядок здійснення державного контролю за дотриманням вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг [240];

- «Про стимулювання розвитку цифрової економіки в Україні» [278] – визначає організаційні, правові та фінансові засади функціонування правового режиму Дія Сіті, що запроваджується з метою стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих умов для ведення інноваційного бізнесу, розбудови цифрової інфраструктури, залучення інвестицій, а також талановитих спеціалістів [278];

- «Про Національну програму інформатизації» [265] – регулює правові відносини, що виникають під час формування та виконання Національної програми інформатизації, в якій, серед іншого, зазначається, що адміністрування засобу інформатизації є видом управлінської діяльності власника та/або технічного адміністратора засобу інформатизації під час експлуатації засобу, спрямований на забезпечення керованості (управління) таким засобом інформатизації та/або його доступності для користувачів інформаційно-комунікаційних систем і засобів інформатизації;

- «Про цифровий контент та цифрові послуги» [288] – регулює відносини між виконавцем та споживачем щодо надання цифрового контенту та/або цифрової послуги. Дія цього Закону поширюється також на: відносини, в яких виконавець на підставі договору надає або зобов'язується надати цифровий контент та/або цифрову послугу споживачу, а споживач надає або зобов'язується надати свої персональні дані, крім випадків, якщо їх надання необхідне виключно для одержання цифрового контенту та/або цифрової послуги, без наміру подальшого використання персональних даних для досягнення будь-яких інших цілей; відносини, в яких цифровий контент та/або цифрові послуги розробляються відповідно до специфікації споживача;

відносини, в яких виконавець на підставі договору надає або зобов'язується надати цифровий контент на матеріальному носії, що використовується виключно для зберігання такого цифрового контенту [288];

- «Про ратифікацію Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027)» [275] – у відповідності до вказаної Угоди Україна бере участь у програмі «Цифрова Європа» згідно з принципами та умовами, встановленими статтею 451 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом і його державами-членами, з іншої сторони, і Протоколом III до неї, Регламентом (ЄС) 2021/694, а також будь-якими іншими нормативно-правовими актами, що стосуються реалізації програми «Цифрова Європа», в їхніх останніх редакціях, і відповідно до конкретних умов, передбачених цією Угодою. Юридичні та фізичні особи, які зареєстровані в Україні, можуть брати участь у заходах програми «Цифрова Європа» на умовах, рівнозначних тим, що застосовуються до юридичних та фізичних осіб, які зареєстровані у Європейському Союзі, з урахуванням дотримання обмежувальних заходів Європейського Союзу [275].

Адміністративно-правовими засадами цифровізації публічного управління та використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності є наступні підзаконні нормативно-правові акти:

- «Засади реалізації органами виконавчої влади принципів державної політики цифрового розвитку», затверджені постановою Кабінету Міністрів України від 30 січня 2019 р. № 56 [96] – визначають принципи реалізації органами виконавчої влади державної політики цифрового розвитку (застосування принципів державної політики цифрового розвитку під час реалізації прав та свобод громадян забезпечується органами виконавчої влади в процесі підготовки проектів нових нормативно-правових актів або внесення змін до нормативно-правових актів і реалізації владних повноважень шляхом застосування цифрових технологій). Так, у відповідності до зазначеної постанови Кабінету Міністрів України, реалізація державної політики

цифрового розвитку ґрунтується на принципах: відкритості (передбачає забезпечення відкритого доступу до відомчих даних (інформації), якщо інше не встановлено чинним законодавством); прозорості (передбачає забезпечення можливості використання відкритих зовнішніх інтерфейсів до відомчих інформаційних систем, включаючи інтерфейси прикладного програмування); багаторазовості використання (передбачає забезпечення відкритого міжвідомчого обміну рішеннями та їх повторного використання); технологічної нейтральності і портативності даних (передбачає забезпечення доступу до відомчих сервісів і даних та повторного використання незалежно від технологій або їх продуктів); орієнтованості на громадян (передбачає забезпечення першочергового врахування потреб та очікувань громадян під час прийняття рішень щодо форм чи способів здійснення функцій держави); інклюзивності та доступності (передбачає забезпечення можливості для всіх громадян користуватися новітніми досягненнями інформаційних технологій доступу до сервісів); безпечності та конфіденційності (передбачає забезпечення для громадян і суб'єктів господарювання безпечного та надійного середовища, в якому відбувається електронна взаємодія з державою, включаючи повну відповідність вказаного середовища правилам і вимогам, встановленим законами України щодо захисту персональних даних та інформації, що належить державі, електронної ідентифікації та довірчих послуг); багатомовності (передбачає забезпечення надання громадянам і суб'єктам господарювання адміністративних, інформаційних та інших послуг, включаючи транскордонні, з використанням мови за їх вибором); підтримки прийняття рішень (передбачає забезпечення використання новітніх інформаційних технологій для розроблення програмних продуктів, які підтримують прийняття рішень органами публічної адміністрації під час реалізації владних повноважень); адміністративного спрощення (передбачає забезпечення прискорення та спрощення адміністративних процесів шляхом їх цифрового розвитку); збереження інформації (передбачає забезпечення зберігання рішень, інформації, записів та даних, достовірності та цілісності, а

також їх доступності відповідно до політики безпеки та конфіденційності протягом певного часу); оцінювання ефективності та результативності (передбачає проведення всебічного оцінювання та порівняння не менш як двох альтернативних рішень для забезпечення ефективності та результативності реалізації владних повноважень) [96];

- «Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року», схвалена розпорядженням Кабінету Міністрів України від 17 листопада 2021 р. № 1467-р. [282];

- «Стратегія цифрової трансформації соціальної сфери», схвалена розпорядженням Кабінету Міністрів України від 28 жовтня 2020 р. № 1353-р [286];

- «Концепція розвитку цифрових компетентностей», схвалена розпорядженням Кабінету Міністрів України від 3 березня 2021 р. № 167-р. [280] – основними проблемами з питань розвитку цифрових компетентностей, які потребують розв'язання в рамках цієї Концепції, є відсутність: правового регулювання питань розвитку цифрових компетентностей; системи та опису цифрової компетентності (рамки цифрової компетентності), а також вимог до рівнів володіння цифровими навичками та цифровими компетентностями різних категорій працівників; єдиних підходів до визначення цифрових компетентностей у професійних стандартах та єдиних вимог до освітніх програм з розвитку інформаційно-цифрової компетентності фахівців різних професій; єдиних вимог до цифрових компетентностей в системі освіти; вимог до цифрової компетентності в професійних стандартах; системи індикаторів для моніторингу стану розвитку цифрових навичок та цифрових компетентностей; координації дій на рівні органів виконавчої влади та органів місцевого самоврядування під час реалізації державної політики у сфері розвитку цифрових навичок та цифрових компетентностей; системи сертифікації рівня цифрових компетентностей [280];

- «Концепція розвитку штучного інтелекту в Україні», схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. [281].

Таким чином, в Україні створено достатньо потужну основу цифровізації суспільних відносин, включаючи відносини у сфері публічного управління та забезпечення безпеки життєдіяльності.

Серед нормативно-правових актів, якими безпосередньо регламентовано впровадження та використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, слід виділити наказ МВС України від 04.05.2016 № 356 «Про затвердження Положення про підсистему реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт єдиної державної системи цивільного захисту» [186] та наказ МВС України від 20.04.2023 № 326 «Про затвердження Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ» [255].

Проте, адміністративно-правової регламентації потребує ще значна кількість суспільних відносин, пов’язаних із використанням інформаційних технологій у сфері забезпечення безпеки життєдіяльності, серед яких, відносини щодо залучення добровольців для ліквідації надзвичайних ситуацій з використанням можливостей мобільних застосунків; відносини, пов’язані із використанням технології штучного інтелекту для удосконалення єдиної державної системи цивільного захисту та механізму забезпечення безпеки життєдіяльності в цілому тощо.

Сучасні інформаційні технології розвиваються із надзвичайною швидкістю, адже над їх створенням працюють провідні корпорації світу, в їх розробку вкладаються мільярди доларів. Водночас створення та впровадження в реальне життя інноваційних інформаційних технологій часто потребує узгодження із існуючим механізмом захисту прав і свобод людини, адже цифрові інструменти дозволяють швидко збирати, аналізувати та

систематизувати інформацію, включаючи персональну інформацію про людину, її особисте життя, а також інформацію, яка становить комерційну чи державну таємницю.

До таких технологій відноситься зокрема і технологія штучного інтелекту, яка має здатність до саморозвитку, самовдосконалення, функціонування без участі людини-оператора.

Інструментарій штучного інтелекту має значний потенціал для полегшення життя людини, адже дозволяє виконувати ті функції, які раніше міг виконувати лише спеціально підготовлений спеціаліст – фізична особа із відповідною кваліфікацією, рівнем освіти та досвідом роботи.

Особливої актуальності використання технології штучного інтелекту набуває у сфері забезпечення безпеки життєдіяльності, адже цифрові інструменти штучного інтелекту дозволяють здійснювати неупереджений моніторинг стану навколишнього природного середовища, стану дотримання правил безпеки на підприємствах, включаючи об’єкти критичної інфраструктури. Технологія штучного інтелекту може забезпечити миттєве реагування на надзвичайну ситуацію, яка виникає внаслідок аварії техногенного чи природного характеру, а також забезпечити швидку мобілізацію людських та матеріально-технічних ресурсів для ліквідації надзвичайної ситуації та її наслідків.

Водночас, використання технології штучного інтелекту потребує належного правового врегулювання, адже у сфері цивільного захисту будь-яка технічна помилка може призвести до непередбачуваних або навіть катастрофічних наслідків. Наприклад, внаслідок несанкціонованого втручання в роботу автоматизованої системи або програмного збою не спрацює протипожежна сигналізація, система радіаційного чи хімічного захисту тощо.

Тому в адміністративно-правових актах повинні бути чітко прописані регламенти використання технології штучного інтелекту, роль людини-оператора, яка буде здійснювати контроль роботи штучного інтелекту, а також прописані ті засоби забезпечення безпеки життєдіяльності, для практичної

реалізації яких не можуть бути застосовані інструменти штучного інтелекту (потрібен повний контроль з боку людини).

Вищезазначене обумовлює окрему увагу до адміністративно-правових засад використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності.

Отже, однією з останніх розробок у сфері інформаційних технологій є технологія штучного інтелекту, яка передбачає самостійну обробку інформації комп'ютером за визначеними алгоритмами, результатом чого є систематизація наявної в мережі інформації, а також створення нових цифрових товарів за допомогою комбінації та синтезу доступних елементів (зображень, відеофайлів, аудіозаписів, текстів тощо).

Технологія штучного інтелекту природно привертає увагу науковців, зокрема і в сфері юриспруденції. Із останніх наукових праць, присвячених різним аспектам правового регулювання використання технології штучного інтелекту, слід відзначити публікації О. Кузьменко, В. Чорної та С. Островського на тему «Правове регулювання запровадження та використання штучного інтелекту» [157], О. Кожухар «Правове регулювання систем штучного інтелекту в ЄС: передумови, сучасний стан та перспективи» [144], В. Бойко «Правове регулювання штучного інтелекту: міжнародний досвід» [35], О. Куракіна та О. Скрябіна «Особливості правового регулювання використання штучного інтелекту в Україні» [159], Ю. Муравської та Т. Сліпченко «Правове регулювання штучного інтелекту в Україні та світі» [182], О. Співака «Правові засади регулювання штучного інтелекту в Україні та Польщі» [302], Д. Позової «Перспективи правового регулювання штучного інтелекту за законодавством ЄС» [218].

Так, Кузьменко, В. Чорна та С. Островський зазначать, що питання правового регулювання діяльності штучного інтелекту вимагає комплексного підходу, який би забезпечував не тільки захист прав людини та суспільних інтересів, але й сприяв подальшому розвитку та інтеграції інноваційних технологій. Розробка та впровадження ефективного правового механізму,

здатного адаптуватися до швидких технологічних змін, стане ключовим завданням для юристів, законодавців та всього міжнародного співтовариства. Також науковці зазначають, що впровадження правового регулювання штучного інтелекту є критично важливим для забезпечення його безпечного та етичного використання. Міжнародна співпраця та гармонізація нормативних рамок можуть сприяти створенню ефективної системи регулювання, що враховує інтереси всіх сторін і сприяє розвитку інновацій, одночасно захищаючи права та свободи людини [157, с. 177].

Таким чином, законодавче врегулювання використання технології штучного інтелекту необхідне, у тому числі, і для забезпечення безпеки життєдіяльності, тобто захисту кожної людини та суспільства в цілому від можливих негативних наслідків використання технології штучного інтелекту.

О. Кожухар зауважує, що Україна нині перебуває в ситуації, коли системи штучного інтелекту вже активно використовуються, зокрема, органами державної влади. Впровадження технологій штучного інтелекту відбувається в умовах, коли розроблення правового регулювання, дотичного до використання систем штучного інтелекту, перебуває на початкових етапах. Також О. Кожухар констатує, що у зв'язку із впровадженням систем штучного інтелекту Україна зіткнулася з комплексними та міждисциплінарними викликами, які охоплюють багато питань. Йдеться не лише про регулювання використання систем штучного інтелекту, а й узгодження національної нормативно-правової бази суміжних сфер із сучасними вимогами та стандартами, зокрема зі стандартами ЄС (наприклад, у сфері захисту персональних даних) [144, с. 71].

Отже, на даний час органи публічної адміністрації використовують технологію штучного інтелекту за відсутності належної законодавчої основи, що певним чином протирічить положенням ст. 19 Конституції України, згідно з якими «органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України».

На думку В. Бойко, штучний інтелект нині стає невід'ємною складовою сучасного світу, проникаючи в різні сфери, зокрема публічне управління та адміністрування. Завдяки своїй здатності обробляти великі обсяги даних та розв'язувати складні завдання, штучний інтелект може відзначитися значним підвищенням ефективності у процесі ухвалення рішень у цих галузях. Проте швидкий технологічний розвиток штучного інтелекту вимагає відповідного правового регулювання, спрямованого на його ефективне та етичне використання. У зв'язку з тим, що в Україні поки не існує спеціалізованого законодавства у цій області, важливо вивчити міжнародний досвід та використовувати його при формуванні вітчизняного законодавства [35, с. 23].

В цілому слід погодитись із такою позицією, адже Україна прагне набути повноправного членства в Європейському Союзі, що вимагає від національних органів публічної адміністрації активізації зусиль щодо адаптації національного законодавства до принципів та норм права ЄС, включаючи сферу адміністративно-правового регулювання використання та розвитку інформаційних технологій, до яких відноситься і технологія штучного інтелекту.

О. Куракін та О. Скрябін справедливо зазначають, що правове регулювання використання штучного інтелекту в Україні знаходиться на стадії розробки: зроблені перші кроки нормативно-правового регулювання використання штучного інтелекту – схвалено Концепцію розвитку штучного інтелекту, презентована Дорожня карта регулювання штучного інтелекту, розроблена «Стратегія розвитку штучного інтелекту в Україні на 2022-2030», прийнятий Закон «Про авторське право та суміжні права». Зважаючи на стрімкий розвиток технологій штучного інтелекту, на думку О. Куракіна та О. Скрябіна, доцільним є комплексний підхід, що буде враховувати всі аспекти використання технологій штучного інтелекту. На їх думку, важливо прийняти Закон про штучний інтелект, який буде встановлювати норми щодо визначення правосуб'єктності систем штучного інтелекту, етичні аспекти використання технологій штучного інтелекту, охоплювати різні сфери

використання штучного інтелекту, визначати права та обов’язки при використанні таких технологій та відповідальність за порушення цих норм [159, с. 40].

У зв’язку із вищевикладеним слід зазначити, що в умовах швидкого розвитку інформаційних технологій важко передбачити перспективи розвитку технології штучного інтелекту у 2022-2030 роках, а також планувати правове регулювання використання вказаної технології на майбутнє. Питання прийняття спеціального закону про штучний інтелект є актуальним вже сьогодні і вже зараз необхідно визначити основні правила використання вказаної інформаційної технології у різних сферах суспільних відносин, включаючи забезпечення безпеки життєдіяльності.

На думку Ю. Муравської та Т. Сліпченко, «регулювання штучного інтелекту сьогодні керується корпоративними інтересами і підтримується етичним підходом. Водночас етичні рамки помітно відрізняються від правових рамок, враховуючи, що правові рамки можуть розроблятися тільки міжнародними законодавчими органами або законодавчими органами держав. Крім того, етичні правила обов’язкові лише у вузькому контексті та тягнуть за собою, у випадках їх недотримання, морально-етичне покарання, а правові норми є обов’язковими у глобальному контексті, а їх недотримання тягне за собою адміністративну, цивільно-правову та кримінальну відповідальність» [182, с. 193].

Також Ю. Муравська та Т. Сліпченко зазначають, що «у правовому регулюванні штучного інтелекту на сьогодні існує кілька нормативних проблем, через які завдання здається нездійсненним. Традиційно нові технології випереджають закон. Однак, якщо регулюючі органи працюватимуть над всебічним розумінням технології, пов›язаної зі штучним інтелектом, у напрямку формування системи нормативно-правового регулювання, потенційно буде розроблене ефективне законодавство про штучний інтелект» [182, с. 193].

Варто погодитись із тим, що етичних норм недостатньо для регулювання всіх аспектів використання технології штучного інтелекту, адже використання вказаної інформаційної технології часто пов’язане із необхідністю дотримання прав і свобод людини, зокрема, права особи на таємницю особистого життя, права на захист персональних даних тощо.

О. Співак зазначає, що порівняльно-правовий аналіз законодавства України та Польщі показав, що питання правових засад регулювання штучного інтелекту перебувають на етапі становлення в обох державах. Враховуючи чимало прогалин та тільки становлення правових концепцій щодо розуміння можливості застосування штучного інтелекту, притягнення до цивільно-правової та іншої відповідальності, вкрай важливим є розробка в обох державах спеціальних законодавчих актів [302, с. 816-817].

Слід зазначити, що одним із ключових питань правового регулювання використання технології штучного інтелекту є якраз питання юридичної відповідальності за наслідки використання вказаної інформаційної технології. Зокрема, точаться дискусії щодо суб’єкта такої відповідальності, яким може бути як розробник конкретної технології штучного інтелекту, так і її користувач, який створив новий цифровий контент, використовуючи штучний інтелект із протиправною метою. Наприклад, наслідком використання штучного інтелекту стало створення забороненого законодавством контенту, або розголошення персональних даних чи комерційної таємниці без відповідної згоди.

Також варто погодитись із позицією Д. Позової, яка зазначає, що розробка певних європейських правових стандартів відносно робототехніки і штучного інтелекту сприятиме розвитку відповідної галузі та забезпечить дотримання прав людини при формуванні нових суспільних відносин за участю автономних пристроїв [218, с. 119].

Таким чином, майже всі науковці приходять до висновку, що існує об’єктивна потреба у розробці та прийнятті спеціального закону, яким будуть

врегульовані основні аспекти використання технології штучного інтелекту у різних суспільних відносинах.

Технологія штучного інтелекту потенційно може замінити людину у багатьох сферах виробництва, обслуговування та навіть у сфері інтелектуальної творчості.

Деякі користувачі Інтернет навіть висловлюють побоювання, що штучний інтелект, здатний до самонавчання, врешті решт може прийняти рішення про те, що можна завдати шкоди людині або навіть знищити людство. Проте такі страхи здебільшого навіяні незнанням самої природи нової інформаційної технології. Адже алгоритми, за якими працює штучний інтелект, створюються людиною, а саме, програмістами, які розробляють відповідне програмне забезпечення. Отже, штучний інтелект може досягати лише тих цілей, які поставив перед ним розробник. Так, технологія штучного інтелекту вже використовується в безпілотних літальних апаратах військового призначення – дронах з машинним зором, метою яких є пошук запрограмованого образу противника та його знищення.

Таким чином, штучний інтелект є загрозою безпеці життєдіяльності людини лише тоді, коли він спеціально створений та налаштований на завдання шкоди іншим людям, як правило, в рамках військових компаній.

Водночас, інструментарій штучного інтелекту дозволяє достатньо широко використовувати цю новітню інформаційну технологію у сфері забезпечення безпеки життєдіяльності.

Так, штучний інтелект за заданими алгоритмами може аналізувати інформацію з датчиків, які розміщені на об’єктах критичної інфраструктури, небезпечних виробництвах, і надходить до єдиного аналітичного дата-центру. В такому випадку штучний інтелект може частково замінити людину-оператора відповідної системи безпеки. Саме частково, тому що фінальний контроль повинна здійснювати саме людина, адже ніхто не може гарантувати неможливість навмисного несанкціонованого втручання в роботу штучного

інтелекту шляхом поширення шкідливого програмного забезпечення, викривлення даних, які отримує комп’ютер для обробки тощо.

До прикладу, штучний інтелект цілком може здійснювати нагляд за безпекою дорожнього руху, аналізуючи записи з дорожніх відеокамер і у разі загрози виникнення аварійної ситуації автоматично перекривати рух, перенаправляти потоки транспорту, здійснювати виклик аварійної бригади, швидкої допомоги, поліції та пожежників.

Так само штучний інтелект може бути використаний в протипожежних автоматизованих системах, забезпечуючи багатофакторний аналіз стану протипожежної безпеки та інформуючи людину-оператора про наявні загрози та проблеми.

Також засобами штучного інтелекту можливо здійснювати прогнозування виникнення надзвичайних ситуацій, причиною яких є стихійні природні лиха та техногенні катастрофи.

На об’єктах, пов’язаних із можливістю радіаційного забруднення територій, остаточний контроль за обладнанням вказаних об’єктів повинна здійснювати людина, точніше група людей, які несуть персональну відповідальність за стан безпеки та знімають (фіксують) показники автоматизованих систем контролю. Так, наприклад, на атомних електростанціях технології штучного інтелекту не можна довірити тотальний та остаточний контроль роботи реакторів та супутнього обладнання, зокрема, автоматизованих систем радіаційного контролю, адже у випадку програмного збою або несанкціонованого втручання в роботу автоматизованих систем, що призведе до неконтрольованого витоку радіації (радіоактивного зараження), наслідки для територій та населення будуть катастрофічними. Більше того, фактично ніхто не нестиме відповідальність за вказані катастрофічні наслідки, хіба що розробник відповідної технології штучного інтелекту.

Окремо слід наголосити на необхідності адміністративно-правового регулювання використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності. Належна правова регламентація

повинна забезпечити однаковий (стандартизований) підхід до використання інструментарію штучного інтелекту суб'єктами владних повноважень органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, керівниками та уповноваженими посадовими особами підприємств, установ та організацій незалежно від форми власності. Однаковий підхід повинен забезпечити сумісність програмного забезпечення, а також унеможливити несанкціоноване втручання в роботу штучного інтелекту в чутливих сферах суспільних відносин, пов'язаних із забезпеченням безпеки життєдіяльності, тобто з високим ризиком завдання шкоди населенню чи природному середовищу.

В Україні наразі відсутнє належне правове регулювання використання технології штучного інтелекту, відповідні проєкти нормативно-правових актів знаходяться на стадії розробки. На даний час прийнятий лише програмний документ загального характеру. Так, Концепція розвитку штучного інтелекту в Україні схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 року № 1556-р.

У відповідності до вказаної Концепції, 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 [281].

Крім того, як було зазначено вище, презентована Дорожня карта регулювання штучного інтелекту та розроблена «Стратегія розвитку штучного інтелекту в Україні на 2022-2030».

Водночас в Європейському Союзі 01 серпня 2024 року набув чинності схвалений Європейським парламентом і Радою ЄС Закон (Акт, Регламент) про штучний інтелект (Artificial Intelligence Act, AI Act) [184].

Так, офіційний журнал ЄС опублікував вказаний Регламент (UE) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року.

Вказаний Закон надає розробникам і користувачам систем чіткі вимоги та зобов'язання щодо конкретного використання штучного інтелекту, одночасно зменшуючи адміністративний і фінансовий тягар для бізнесу [184].

В. Місечко зазначає, що Artificial Intelligence Act (AI Act) експерти називають еталоном у сфері регулювання технологій та систем штучного інтелекту і прогнозують, що на нього будуть рівнятися законотворці усіх держав світу. Його сфера дії охоплює всі сектори економіки (за винятком військового) та всі типи штучного інтелекту. На його думку, українцям важливо розібратися в положеннях закону про штучний інтелект насамперед з наступних причин: оскільки Україна впевнено крокує до вступу в Євросоюз, найближчими роками норми AI Act будуть імплементовані в наше законодавство; нормам AI Act повинні відповідати всі системи штучного інтелекту, які бажають отримати доступ до внутрішнього ринку ЄС, тобто їх мають дотримуватися відповідно українські розробники та постачальники для транскордонного надання послуг і продуктів, пов'язаних зі штучним інтелектом [179].

Юристи патентно-правової фірми «Пахаренко і партнери» зазначають, що європейський Закон про штучний інтелект не буде застосовуватися в цілому до 2 серпня 2026 року, протягом 24 місяців з моменту набуття ним чинності, але деякі його положення будуть застосовуватися в різний час, а саме: заборона на певні практики, пов'язані зі штучним інтелектом, почне діяти з 2 лютого 2025 року; положення, що стосуються нотифікованих органів, моделей штучного інтелекту загального призначення, які створюють системні ризики, системи управління штучним інтелектом в Європі та значної частини набору санкцій, будуть застосовуватися з 2 серпня 2025 року; регулювання певних систем штучного інтелекту з високим ризиком (компонентів безпеки продуктів або тих, які самі є продуктами та вимагають оцінки відповідності для розміщення на ринку або введення в експлуатацію, наприклад машин, іграшок, ліфтів або медичних пристроїв) передбачено застосовувати з 2 серпня 2027 року [187].

Таким чином, перед науковцями та органами публічної адміністрації в Україні нагальним є завдання розробити та прийняти відповідний національний закон про штучний інтелект, яким будуть врегульовані всі можливі аспекти використання даної інформаційної технології у різних сферах суспільних відносин, включаючи сферу забезпечення безпеки життєдіяльності. Деталізоване правове регулювання відповідних правовідносин доцільно забезпечити на рівні постанов Кабінету Міністрів України та підзаконних, відомчих нормативно-правових актів.

За результатами проведеного аналізу слід наголосити на необхідності внесення змін до чинного національного адміністративного законодавства в частині правової регламентації використання інструментарію технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності. Зокрема, доцільно розробити та прийняти відповідний національний закон про штучний інтелект, яким будуть врегульовані всі можливі аспекти використання даної інформаційної технології у різних сферах суспільних відносин, включаючи сферу забезпечення безпеки життєдіяльності.

Під час розробки відповідного законопроекту доцільно враховувати положення європейського закону (акту) про штучний інтелект (Artificial Intelligence Act, AI Act), що відповідає загальній політиці національного уряду щодо адаптації національного законодавства до права ЄС.

На окрему увагу заслуговує питання правового регулювання та матеріально-технічного забезпечення цифровізації систем цивільного захисту та безпеки життєдіяльності.

Результатом розвитку інформаційних технологій стала поява широкого спектру цифрових інструментів, які дозволяють значно покращити людське життя. Серед іншого, інформаційні технології є засобом удосконалення публічного управління та адміністрування суспільних відносин. Однією із сфер публічного управління, в якій інформаційні технології відіграють ключову роль, є сфера забезпечення безпеки життєдіяльності, що включає систему цивільного захисту.

Цифровізація вказаної сфери суспільних відносин потребує належного правового регулювання, адже у відповідності до спеціально-дозвільного принципу правового регулювання посадовим особам органів публічної адміністрації дозволено лише те, що прямо передбачено законом. Не менш важливим є належне матеріально-технічне забезпечення використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Інноваційні інформаційні технології потребують комп'ютерного обладнання відповідного рівня, надійних засобів захисту інформації, забезпечення декількох альтернативних засобів зв'язку, особливо у випадках настання надзвичайної ситуації, що супроводжується обривом комунікацій, руйнуванням критичної та цивільної інфраструктури.

Враховуючи вищезазначене, дослідження актуальних питань правового регулювання та матеріально-технічного забезпечення цифровізації систем цивільного захисту та безпеки життєдіяльності має як теоретичне, так і практичне значення для удосконалення чинного національного законодавства та юридичної практики його застосування.

В сучасному високотехнологічному світі все більше уваги приділяється питанням забезпечення безпеки життєдіяльності, адже людину оточує велика кількість потенційно небезпечних чинників (загроз) природного та техногенного характеру, до яких додаються загрози виникнення нових соціальних конфліктів. Особливої актуальності питання забезпечення безпеки життєдіяльності в Україні набуло із початком повномасштабної збройної агресії російської федерації проти України. Систематичні обстріли та ракетні атаки призводять до виникнення надзвичайних ситуацій воєнного характеру, що вирізняються складністю ліквідації та необхідністю взаємодії з військовими.

Забезпечення безпеки життєдіяльності є одним із основних завдань органів публічної адміністрації, адже від якості виконання такого завдання залежить нормальне функціонування та розвиток суспільства, життя та здоров'я громадян, якість життя в цілому. Складовою механізму забезпечення

безпеки життєдіяльності є цивільний захист суспільства та навколишнього природного середовища від надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру. Якщо система цивільного захисту спрямована на ліквідацію надзвичайних ситуацій, то забезпечення безпеки життєдіяльності стосується всіх небезпек для людини та суспільства в цілому.

Безпека життєдіяльності охоплює всі суспільні відносини, досліджуючи існуючі та потенційні небезпеки та загрози існуванню людини, правила відносин між людиною та навколишнім природним та штучним середовищем, включаючи зокрема: правила безпеки поводження із різними речовинами та матеріалами, правила безпеки на виробництві та в інших сферах трудової діяльності людини (норми охорони праці), правила поводження із технічними засобами (інструкції до обладнання, електричних приладів тощо), правила поведінки на воді, правила дорожнього руху, норми безпечності харчових продуктів та продовольчої сировини, правила пожежної безпеки та інші правила, які регулюють відносини людини з навколишнім природним середовищем та рукотворним світом.

Таким чином, норми безпеки життєдіяльності більшою мірою представлені технічними та техніко-юридичними нормами. Перевагою останніх є їх санкціонованість державою, тобто встановлення дисциплінарної, адміністративної або кримінальної відповідальності за їх порушення.

Закріплення технічних норм в нормативно-правових актах надає їм загальнообов’язкового характеру та поширює їх дію на територію всієї держави. Саме тому порядок використання будь-яких нових технологій, які пов’язані із необхідністю встановлення правил безпеки життєдіяльності, доцільно закріплювати на рівні законів або підзаконних нормативно-правових актів.

В сучасному інформаційному суспільстві ключову роль в забезпеченні безпеки життєдіяльності відіграють цифрові технології. Так, завдяки інноваційним інформаційним технологіям функціонують автоматизовані системи моніторингу якості води та повітря, рівня радіаційного забруднення

територій, стану сейсмічної та вулканічної активності, а також автоматичні протипожежні системи, системи технологічного контролю на виробництвах та інші технічні засоби запобігання та ліквідації надзвичайних ситуацій та їх наслідків.

Автоматичні датчики передають інформацію до інформаційних центрів, де відбувається аналіз даних та повідомлення оператора про перевищення допустимих норм, або у випадку перевищення норм система спрацьовує автоматично, активуючи технічні засоби ліквідації надзвичайної ситуації.

Завдяки інформаційним технологіям значно удосконалені засоби комунікації між центральними та регіональними органами публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, а також керівниками підприємств, установ та організацій, які є відповідальними за цивільний захист. Крім того, нові технології дозволяють вести цілодобове відеоспостереження за місцем локалізації надзвичайної ситуації та роботою рятувальників завдяки нагрудним камерам та пересувним і стаціонарним камерам зовнішнього відеоспостереження.

Значний потенціал у сфері забезпечення безпеки життєдіяльності мають соціальні мережі та месенджери. Так, за допомогою соціальних мереж доцільно здійснювати поширення базових знань про засади безпеки життєдіяльності та цивільного захисту, зокрема, розміщувати в порядку реклами правила поведінки в надзвичайних ситуаціях, правила поводження із небезпечними предметами та речовинами, правила евакуації при пожежах, повенях, ракетних атаках тощо. Причому, завдяки можливостям веб-дизайну, названі правила доцільно розміщувати у вигляді анімаційних роликів, відео-сюжетів, інтерактивних таблиць та карт, ярких схем та банерів. В свою чергу, за допомогою соціальних месенджерів можливо розсилати повідомлення про надзвичайні ситуації та їх наслідки, інформацію про засоби зв’язку із рятувальними службами та щодо пунктів незламності.

Офіційні сторінки ДСНС України в соціальних мережах повинні мати максимальне інформаційне наповнення, містити інтерактивні карти укриттів,

захисних споруд з можливістю навігації (побудови маршруту до них з урахуванням геолокації, місцезнаходження користувача), засоби відеозв'язку з черговими операторами ДСНС в режимі онлайн, які мають функціонувати цілодобово. У випадку, якщо особа опинилася в епіцентрі надзвичайної ситуації чи постраждала від її негативних наслідків, вона повинна мати можливість зв'язатися із оператором ДСНС через відповідний месенджер та отримати невідкладну інформаційну допомогу, поради щодо поведінки та напрямів евакуації, надання первинної медичної допомоги постраждалим тощо. В свою чергу, спеціаліст ДСНС зможе не тільки координувати дії постраждалої особи, але й надавати їй психологічну підтримку в екстремальній ситуації.

В соціальних мережах та месенджерах також передбачена можливість створення спеціалізованих груп для обміну інформацією про надзвичайні події, включаючи фото та відео-повідомлення. Адмініструвати такі групи можуть як спеціалісти ДСНС, так і прості громадяни-добровольці в координації з фахівцями ДСНС України.

Важливу роль в ліквідації надзвичайних ситуацій та їх наслідків відіграють роботизовані технічні засоби, які можуть проникати на ті ділянки уражених, пошкоджених об'єктів, де перебування людини є небезпечним. Роботи застосовуються, зокрема, для дистанційного розмінування територій та об'єктів нерухомості, проведення робіт на об'єктах, які опинилися в зоні радіоактивного забруднення тощо. Для проведення перелічених робіт застосовуються як наземні дрони, так і безпілотні літальні апарати.

Також для удосконалення механізму забезпечення життєдіяльності активно використовуються мобільні застосунки, які дозволяють оперативно інформувати громадян про надзвичайні події та ситуації, надавати поради та інформацію щодо розташування найближчих укриттів, захисних споруд тощо. Позитивними прикладами застосування такої технології є мобільний застосунок «Повітряна тривога» та чат-бот «Укриття». Крім того, на даний час проходить тестові випробування нова Система оповіщення та реагування «Я –

доброволець» з відповідним мобільним застосунком, яка сприятиме залученню громадян-добровольців до ліквідації надзвичайних ситуацій та їх наслідків. Так, кожен громадянин України зможе за допомогою вказаного мобільного застосунку долучитися до єдиної інформаційної бази добровольців, надати дозвіл на визначення координат свого місцезнаходження та отримувати на свій смартфон повідомлення про надзвичайні ситуації, які виникли поблизу. Відповідно, співробітники ДСНС України, які адмініструють зазначений мобільний застосунок, зможуть підтримувати інформаційний контакт з добровольцями, які прибули на місце події, надавати поради та координувати їх діяльність. Таким чином, громадяни зможуть проявити соціальну активність, а рятувальники отримують можливість мобілізувати людські та матеріально-технічні ресурси для ліквідації надзвичайних ситуацій та їх наслідків.

Використання та поширення перелічених інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту потребує належного адміністративно-правового врегулювання та матеріально-технічного забезпечення. Закріплення в нормативно-правових актах порядку використання певної інформаційної технології забезпечує уніфікований підхід до її використання, сумісність програмного забезпечення, централізований захист інформаційних ресурсів, а також поширення позитивного локального досвіду використання інформаційних технологій у вказаній сфері суспільних відносин на територію всієї держави.

Крім того, у відповідності до ст. 19 Конституції України, органи державної влади та органи місцевого самоврядування, їх посадові особи зобов’язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України [149]. Таким чином, використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності уповноваженими особами органів публічної адміністрації повинно мати чітку правову основу.

Отже, в Україні існує нагальна потреба адміністративно-правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, включаючи використання спеціальних мобільних застосунків, автоматизованих інформаційних систем та технології штучного інтелекту. Не менш важливим є належний рівень матеріально-технічного забезпечення використання цифрових технологій у вказаній сфері суспільних відносин (забезпечення кількох альтернативних засобів підключення до Інтернет, зберігання інформації на декількох альтернативних автономних серверах, оновлення матеріально-технічної бази, включаючи комп'ютерне обладнання, цифрові камери відеоспостереження тощо).

На окрему увагу заслуговує питання захисту персональних даних та інформаційної безпеки у сфері забезпечення безпеки життєдіяльності.

Безпека життєдіяльності є складною комплексною наукою та навчальною дисципліною про різноманітні загрози та небезпеки, які вливають або можуть вплинути на життєдіяльність людини, а також способи та методи запобігання вказаним загрозам та небезпеками, механізми ліквідації надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру.

Однією із сфер суспільних відносин, в якій наразі актуальними є питання забезпечення життєдіяльності, є сфера інформаційних відносин. Цифровізація суспільного життя створила фактично інший, паралельний світ, який визначають як цифрове середовище.

Цифрове середовище включає в себе всі інформаційно-комунікаційні технології, бази даних та цифрові мережі (Інтернет, мережі мобільного зв'язку), цифрові продукти (контент) та послуги. В цифровому середовищі відбувається постійна взаємодія між людьми, обмін масивами інформації, текстовими, аудіо та відеофайлами, здійснюється електронна торгівля та надання цифрових послуг. Фактично створюється цифровий Всесвіт (віртуальний світ), в якому відображається та відтворюється більша частина реальних суспільних відносин.

Людина як учасник цифрових відносин ідентифікує себе через певний обсяг персональних даних, які завантажує в цифрові мережі, включаючи інформацію про особу, її місцезнаходження, банківські рахунки, вподобання (які визначаються або шляхом опитування або самими алгоритмами пошукових систем, коли мережа пропонує особі в якості рекомендацій той контент, який вона найчастіше шукає).

Природньо, що розвиток цифрових технологій призвів до появи окремого виду протиправної діяльності у вигляді вчинення правопорушень із використанням інформаційних технологій, включаючи несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; поширення шкідливого програмного забезпечення (вірусів), спаму; створення дублікатів офіційних сторінок комерційних установ та органів публічної адміністрації тощо.

Метою протиправної діяльності в цифровому середовищі є отримання доступу до персональних даних особи, включаючи банківські рахунки, інформацію про власність, протиправне переслідування особи, а також порушення роботи інформаційних (автоматизованих) систем.

Таким чином, в цифровому середовищі актуальним є забезпечення безпеки життєдіяльності особи, тобто її безпеки в цифровому форматі, адже правопорушення у цифровому середовищі призводять до негативних наслідків в реальному житті – втрати особою фінансових заощаджень та власності, завдання шкоди репутації, порушення порядку нормальної життєдіяльності (неможливості отримати адміністративні послуги, укласти угоду) тощо.

Вищезазначене обумовлює актуальність питань адміністративно-правового регулювання захисту персональних даних та інформаційної безпеки в контексті забезпечення безпеки життєдіяльності.

Захист персональних даних та інформаційна безпека є одними із найбільш актуальних питань в сучасному інформаційному суспільстві. Наразі більшість учасників суспільних відносин є активними користувачами Інтернет через смартфон або персональний комп'ютер. Відбувається обмін великими

масивами інформації, включаючи тестові, аудіо та відеофайли. Пошукові системи підлаштовуються під типові запроси користувачів, в соціальних мережах формуються спільноти, групи за інтересами. Комерційні компанії активно використовують Інтернет для маркетингу, реклами. В свою чергу органи публічної адміністрації представлені офіційними веб-сайтами та надають широкий спектр електронних (цифрових) адміністративних послуг. Крім того, в мережі відбувається обмін службовою інформацією, створюються та активно наповнюються різноманітні державні реєстри та бази даних.

Водночас цифровий формат даних, які розміщуються в реєстрах, соціальних мережах, пересилаються засобами електронної пошти та через мобільні застосунки (месенджери), робить їх відкритими для інших користувачів, які часто переслідують протиправні цілі. Крім того, люди часто добровільно надають персональну інформацію різноманітним інформаційним ресурсам комерційних компаній, банків, державних установ та організацій, і така інформація також часто стає загальнодоступною.

Професійні хакери з легкістю зламують акаунти, створюють дублікати офіційних веб-сторінок комерційних, банківських установ, отримують несанкціонований доступ до державних реєстрів тощо.

Незахищеність персональних даних значною мірою впливає на безпеку життєдіяльності людини та суспільства в цілому, адже заволодіння персональним даними сторонніми особами із протиправною метою може призвести до вкрай негативних наслідків, включаючи отримання зловмисниками доступу до банківських рахунків особи, використання фото та відеоматеріалів для шантажу (з погрозами поширити конфіденційну, інтимну інформацію), створення клонів сторінок певної особи у соціальних мережах та здійснення від її імені певної діяльності (збирання коштів на нібито лікування та інші потреби; здійснення психологічного тиску на родичів та знайомих з метою схилити їх до певних дій; поширення матеріалів, які дискредитують особу тощо). Не поодинокими є випадки здійснення від імені особи,

персональні дані якої викрадено, терористичної діяльності, вчинення інших злочинів проти національної безпеки.

Таким чином, захист персональних даних у сфері забезпечення безпеки життєдіяльності є одним із завдань національних органів публічної адміністрації. Правовою основою виконання даного завдання є Закон України «Про захист персональних даних». Вказаний закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Він поширюється, у тому числі, на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів [260].

В Законі України «Про захист персональних даних» чітко зазначено, що мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством (ст. 6 Закону України «Про захист персональних даних») [260].

Крім того, враховуючи євроінтеграційні прагнення України, важливим є дотримання європейських стандартів у сфері захисту персональних даних.

Так, в Європейському Союзі у 2016 році прийнято Загальний регламент про захист даних (General Data Protection Regulation, GDPR). Цей загальноєвропейський акт суттєво розширює повноваження держав у сфері соціальних мереж – дозволяє видаляти незаконний контент і змушує платформи докладати більше зусиль для боротьби з небезпечними матеріалами [298].

Загальний регламент захисту даних (GDPR) є найсуворішим законом про конфіденційність і безпеку в світі. Незважаючи на те, що він був розроблений і прийнятий в Європейському Союзі, він накладає зобов'язання на підприємства, установи та організації незалежно від місця їх знаходження, якщо вони націлені або збирають дані, пов'язані із громадянами держав-членів ЄС.

Загальний регламент захисту даних (GDPR) набув чинності 25 травня 2018 року. GDPR передбачає стягнення значних за розміром штрафів за порушення стандартів конфіденційності та безпеки, причому штрафи можуть сягати десятків мільйонів євро. За допомогою вказаного акту Європейський Союз демонструє свою тверду позицію щодо необхідності захисту конфіденційності та безпеки даних у той час, коли все більше людей довіряють свої особисті дані хмарним сервісам (службам), а порушення у цій сфері є щоденним явищем [368].

Особливу увагу необхідно приділити питанню захисту персональних даних в процесі використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Так, в Україні наразі відбувається впровадження (тестування) Системи оповіщення та реагування «Я-Доброволець» [296].

Система оповіщення та реагування «Я – доброволець» є інноваційною платформою, яка дозволяє організувати та координувати дії соціально активних громадян, які готові добровільно долучитися до ліквідації надзвичайних ситуацій та їх наслідків, використовуючи свій професійний досвід і навички. Тобто, завдяки додатку для смартфона, кожен охочий може стати на захист своєї громади, отримуючи вказівки та інструкції щодо подолання небезпек. Така платформа також дозволяє вносити всі необхідні відомості про добровольця до інформаційної бази, аби оперативно та своєчасно повідомляти людину про можливість її залучення до ліквідації надзвичайних ситуацій з урахуванням місцезнаходження (геолокації) особи [296].

Отже, враховуючи функціонування загальнодержавної системи цивільного захисту в умовах правового режиму воєнного стану, необхідно забезпечити належний рівень захисту персональних даних добровольців, які вносять відомості про себе в інформаційну базу Системи оповіщення та реагування «Я – доброволець».

На рівні спільного наказу МВС України та Міністерства цифрової трансформації України доцільно затвердити порядок функціонування Системи оповіщення та реагування «Я – доброволець» та заходи щодо криптографічного захисту персональних даних добровольців, які внесені до бази даних вказаної Системи.

На окрему увагу заслуговує питання захисту персональних даних в процесі використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності. Алгоритми штучного інтелекту дозволяють аналізувати великі масиви даних, збирати та систематизувати інформацію з камер зовнішнього відеоспостереження, різноманітну інформацію з Інтернет, включаючи персональні дані. Наприклад, з використанням системи камер відеоспостереження (включаючи як стаціонарні камери, так і камери смартфонів, ноутбуків, відеореєстраторів) та інформації із соціальних мереж за допомогою технології штучного інтелекту може здійснюватися несанкціоноване стеження за певною особою чи групою осіб, що з одного боку полегшує роботу органів безпеки та правопорядку, але з іншого є втручанням в особисте (інтимне) життя людини.

Таким чином, використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності повинно мати чітку правову основу, яка буде передбачати захист персональних даних від несанкціонованого збирання та аналізу.

Безпека життєдіяльності людини у цифровому просторі передбачає також захист від злочинного переслідування особи, що може завдати останній як психологічної травми, так і призвести до більш негативних наслідків – спроби чи вчинення злочину, самогубства тощо.

7 грудня 2017 року Верховною Радою України було прийнято Закон України «Про запобігання та протидію домашньому насильству». Вказаним Законом України було визначено організаційно-правові засади запобігання та протидії домашньому насильству, основні напрями реалізації державної політики у сфері запобігання та протидії домашньому насильству, спрямовані на захист прав та інтересів осіб, які постраждали від такого насильства. Закон активно впроваджується, склалася певна адміністративна та судова практика його застосування.

Водночас в Україні досі законодавчо не врегульовано поняття сталкінгу, тобто злочинного переслідування особи, яке в умовах інформаційного суспільства часто здійснюється з використанням інформаційних технологій. Це, до прикладу, цькування людини в Інтернет, зокрема, в соціальних мережах, поширення про неї неправдивої інформації, незаконне стеження за особою за допомогою цифрових інструментів тощо.

Враховуючи вищезазначене наразі розроблено Проект Закону України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (сталкінг)» у зв’язку з необхідністю удосконалення організаційно-правових засад щодо встановлення відповідальності за злочинне переслідування (сталкінг) та врахування положень Цивільного процесуального кодексу у кримінальному судочинстві в частині застосування обмежувальних заходів щодо осіб, які вчинили домашнє насильство [289].

Вказаним законом пропонується внести зміни до Закону України «Про запобігання та протидію домашньому насильству», зокрема, статтю 1 доповнити пунктами 6 та 7 у яких викласти визначення такого терміну, як злочинне переслідування (сталкінг) та кіберпереслідування [289].

Актуальним також вбачається посилення юридичної відповідальності за кібербулінг.

Так, наразі ст. 173-4 Кодексу України про адміністративні правопорушення передбачає покарання за цькування учасників освітнього процесу у вигляді накладення штрафу до двохсот неоподатковуваних мінімумів доходів громадян або до шестидесяти годин громадських робіт [142]. У разі, якщо психологічне, фізичне, економічне, сексуальне насильство застосувала малолітня або неповнолітня особа, віком від чотирнадцяти до шістнадцяти років, то покарання накладається на їхніх батьків або осіб, які їх замінюють [133].

Якщо ж кривдник, зокрема, шляхом жорстокого поводження, шантажу, систематичного приниження людської гідності або протиправного примусу до небажаних дій, довів жертву до самогубства або замаху до нього, то такі дії передбачають відповідальність за ст. 120 (Доведення до самогубства) Кримінального кодексу України. Санкція статті передбачає до 10 років позбавлення волі [155].

Особі, яка попередньо зламала акаунти жертви для отримання особистої інформації, окрім покарання за булінг, загрожує покарання за ст. 361 (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж) Кримінального кодексу України [133].

Таким чином, очевидною є потреба посилення адміністративної відповідальності за цькування учасників освітнього процесу, включаючи кібербулінг, а також встановлення адміністративної відповідальності за кіберсталкінг, тобто протиправне переслідування особи з використанням інформаційних технологій.

Окремої уваги заслуговує питання інформаційної безпеки в контексті забезпечення безпеки життєдіяльності.

Правовою основою діяльності органів публічної адміністрації в цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави,

національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [269].

Вказаним законом перебачено, серед іншого, функціонування Національної телекомунікаційної мережі (як сукупності спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань) та Національного центру резервування державних інформаційних ресурсів (як організованої сукупності об'єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій) [269].

У відповідності до ст. 6 Закону України «Про основні засади забезпечення кібербезпеки України», розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій [269].

А згідно із ст. 8 вказаного закону національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних,

контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [269].

Слід відзначити, що враховуючи триваючу повномасштабну збройну агресію російської федерації проти України, вразливість національних комунікаційних мереж та серверів, доцільно забезпечити зберігання інформації органів публічної адміністрації на декількох альтернативних серверах, розміщених в зарубіжних країнах, які є надійними партнерами України.

Також слід відзначити важливість Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/202, яка визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [277].

У відповідності до вказаної Стратегії, забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. В Стратегії інформаційної безпеки також справедливо зазначається, що розвиток інформаційного простору в умовах глобалізації та пандемія COVID-19 зумовили посилення ролі соціальних мереж у національному та світовому інформаційному просторі, їх вплив на внутрішню і зовнішню суспільно-політичну ситуацію, стан додержання прав і свобод людини, зокрема щодо забезпечення принципів рівності прав користувачів соціальних мереж.

Хоча право на приватність (захист конфіденційної інформації про особу, невтручання в особисте життя) є одним з основних прав людини, що

закріплено в Загальній декларації прав людини, Конвенції про захист прав людини і основоположних свобод, інших міжнародних документах, а також конституціях більшості держав світу, цифрові трансформації змінюють і цю сферу. Збільшення кількості соціальних мереж, їх інтегрованість з іншими соціальними сервісами повсякденного користування, а також специфіка організації всесвітньої мережі Інтернет ставлять під загрозу гарантії права особи на приватність. Спроби врегулювати цю проблему тривають, формуються нові підходи у забезпеченні балансу права на приватність та інформаційної безпеки держави [277].

Крім того, в Стратегії інформаційної безпеки наголошено на тому, що значне розширення джерел доступу до інформації в умовах стрімкого розвитку цифрових технологій та водночас недостатнього рівня медіаграмотності (медіакультури) супроводжується зменшенням критичності сприйняття інформації, створює підґрунтя для можливих маніпуляцій громадською думкою, що сприяє зростанню впливу дезінформації та деструктивної пропаганди. Некритичне сприйняття інформації створює загрози політичній та економічній стабільності демократичних держав [277].

Крім того, в якості правової основи забезпечення інформаційної безпеки слід відзначити Стратегією кібербезпеки України, затверджену Указом Президента України від 26 серпня 2021 року № 447, в якій зазначено, що питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію [276].

В Стратегії кібербезпеки України підкреслюється, що в сучасному світі зростає технічний рівень реалізації кіберзагроз, постійно вдосконалюються та розробляються нові інструменти і механізми кібератак. Посилюється тенденція щодо використання кібератак як інструменту спеціальних інформаційних операцій, маніпулювання суспільною думкою. Глобального

масштабу набуває використання кіберпростору терористичними організаціями. Пріоритетними цілями кібертероризму є об’єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об’єкти тощо [276].

Таким чином, на вищому державному рівні визнано, що забезпечення інформаційної безпеки та кібербезпеки є найважливішими функціями органів публічної адміністрації, причому кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Отже, система забезпечення безпеки життєдіяльності людини в сучасному світі обов’язково повинна включати механізми захисту персональних даних, забезпечення інформаційної безпеки та кібербезпеки.

Наразі в Україні удосконалено нормативне забезпечення з питань кіберзахисту об’єктів критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту. Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв’язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України. З метою покращення координації діяльності суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері [276].

Таким чином, в Україні створюється адміністративно-правова та інституційна основа забезпечення інформаційної безпеки та кібербезпеки, що сприятиме удосконаленню загального механізму забезпечення безпеки життєдіяльності кожної людини та суспільства в цілому.

Рівень захисту персональних даних та стан інформаційної безпеки напряму впливають на якість забезпечення безпеки життєдіяльності, адже доступність персональних даних та незахищеність інформаційних ресурсів

створюють умови для здійснення протиправної діяльності з використанням інформаційних технологій, зокрема: хакерських атак, шахрайства, протиправного переслідування особи тощо.

З метою удосконалення національних механізмів захисту персональних даних та забезпечення інформаційної безпеки, а також враховуючи євроінтеграційні прагнення України та необхідність адаптації національного законодавства до права Європейського Союзу, доцільно імплементувати в національне законодавство положення європейського Загального регламенту захисту даних (GDPR) та європейського Закону про штучний інтелект (Artificial Intelligence Act, AI Act).

З метою забезпечення інформаційної безпеки у сфері забезпечення безпеки життєдіяльності доцільно зберігати всю службову інформації ДСНС України, а також інформацію про надзвичайні події та їх наслідки, сили та засоби цивільного захисту та іншу важливу інформацію на декількох альтернативних автономних серверах в різних зарубіжних країнах, які мають партнерські відносини з Україною. Також слід підкреслити необхідність багаторівневого, криптографічного захисту інформації у сфері забезпечення безпеки життєдіяльності, якщо вказана інформація становить державну таємницю або її поширення може завдати шкоди національним інтересам України.

4.2 Правові засоби забезпечення безпеки життєдіяльності в контексті цифровізації публічного управління та економіки

Сучасний стан правового регулювання у сфері забезпечення безпеки життєдіяльності потребує удосконалення, адже сучасні інформаційні технології створюють додаткові можливості щодо використання нових інструментів попередження про виникнення надзвичайних ситуацій, а також ліквідації їх наслідків, мобілізації людських та матеріально-технічних ресурсів тощо.

Як відомо, механізм правового регулювання, включаючи правове регулювання у сфері забезпечення безпеки життєдіяльності, складається з правових засобів. В теорії держави і права навіть була створена окрема інструментальна теорія права, яка оперує категорією «правові засоби» для опису фактично всіх правових явищ та процесів, і пропонує розглядати право не як нав'язану державою систему заборон, зобов'язань та дозволів, а як систему дієвих правових інструментів (засобів) досягнення публічної чи приватної мети учасників суспільних відносин.

Враховуючи вищевикладене, дослідження правових засобів забезпечення безпеки життєдіяльності в контексті подальшої цифровізації публічного управління має як теоретичне, так і практичне значення, та є актуальним напрямом наукового пошуку.

Теоретико-методологічною основою дослідження правових засобів забезпечення безпеки життєдіяльності в контексті цифровізації публічного управління є наукові публікації та монографії, присвячені окремим аспектам безпеки життєдіяльності, теорії правових засобів та адміністративно-правовим засадам використання інформаційних технологій у різних сферах суспільних відносин.

На окрему увагу в контексті теми дослідження заслуговують наукові праці, присвячені визначенню поняття та класифікації правових засобів. Серед них варто виділити публікації А. Денисової «Правові засоби: поняття та види.» [91], О. Ганзенка «Теорія правових засобів у контексті інструментальної теорії права» [72], М. Лошицького «Адміністративно-правові засоби в механізмі охорони навколишнього середовища» [169], О. Олійник «Адміністративно-правові засоби забезпечення інформаційної безпеки» [189].

Також слід відзначити, що категорії «правові засоби» та «адміністративно-правові засоби» все більше використовують у своїх дослідженнях вчені-адміністративісти, адже вказані категорії є універсальними і дозволяють аналізувати будь-яке правове явище чи процес з

точки зору інструментальної теорії права, яка вивчає реальні, дієві засоби вирішення певної правової проблеми, колізії тощо.

Правовим засобам у контексті інструментальної теорії права окреме дисертаційне дослідження присвятив О. Онуфрієнко [192].

Так, на думку О. Онуфрієнка, правові засоби – це система субстанціональних та діяльнісних правових явищ, за допомогою яких конкретні суб'єкти правовідносин досягають приватних та публічних цілей [192, с. 14-15].

Наведене визначення є найбільш лаконічним та відображає сутність категорії «правові засоби», причому автор робить акцент на таких цілях правового регулювання як досягнення приватних та публічних цілей, за якими стоять реальні приватні та публічні інтереси фізичних осіб, мотиви їх поведінки, природні та штучні потреби.

А. Денисова визначає правові засоби як правові явища, які відображені в інструментах (постановах) та діях (технологіях), за допомогою яких задовольняються інтереси суб'єктів права, забезпечується досягнення особистих та публічних цілей [91, с. 191-192].

В наведеному визначенні правових засобів також присутні субстанціональні та діяльнісні правові явища, а також інтереси суб'єктів права, особистій та публічні цілі учасників правовідносин.

До ознак правових засобів А. Денісова відносить наступні:

- правові засоби є основними інструментами суб'єктів права для забезпечення особистих та публічних інтересів, досягнення поставлених цілей (до прикладу – людина сприймає нормативно-правові акти не як систему заборон та зобов'язань, а як набір реальних інструментів досягнення приватної чи публічної мети);

- правові засоби відображають соціальну, інструментальну та особистісну цінності права (право в цілому сприймається не як нав'язане державою, а як природний інструментарій задоволення природних та штучних потреб людини та суспільства в цілому);

- правові засоби визначають, певним чином поєднуючись, галузеві правові режими (певна комбінація та співвідношення правових засобів визначає певні методи та типи правового регулювання);

- правові засоби є основними елементами правового впливу, механізму правового регулювання (правові засоби є складовими механізму правового регулювання, утворюючи його правову матерію та визначаючи основні форми та напрями його функціонування);

- правові засоби є спеціальними та загальними засобами, які забезпечують дію правової системи загалом (універсальність категорії «правові засоби дозволяє відносити до них фактично всі правові явища та процеси);

- правові засоби призводять до юридичних наслідків (конкретних результатів, задоволення публічних або приватних інтересів учасників правовідносин);

- правові засоби забезпечують ефективність правового регулювання завдяки постійному взаємозв'язку один з одним (синергетика правових засобів проявляється в реальній практиці правозастосування, коли до тексту нормативно-правового акту додається його тлумачення, судова та адміністративна практика, окрема думка судді тощо);

- правові засоби забезпечуються та підтримуються державою [91, с. 190-191].

Наведені ознаки правових засобів найбільш повно розкривають їх юридичну природу та демонструють універсальність правових засобів як регуляторів суспільних відносин.

За результатами класифікації правових засобів, до субстанціональних правових засобів (засобів-постанов, інструментів) А. Денисова відносить зобов'язання, дозволи, заборони, заохочення, пільги, норми права, принципи права тощо, а до дієвих (засобів-дій, технологій) – акти реалізації права, акти застосування права, акти тлумачення права і всі процеси юридичної

діяльності [91, с. 191-192]. Вченою фактично перелічуються всі елементи механізму правового регулювання, включаючи статичні та динамічні складові.

Всі правові засоби, на її думку, в результаті їх узагальнення (трансформації), поділяються на правові стимули та правові обмеження. Правовий стимул, на її думку, є засобом формування у суб'єкта необхідної законослухняної поведінки шляхом створення необхідних умов щодо задоволення суб'єктивних інтересів завдяки виконанню правових приписів. Водночас правові обмеження є правовим засобом стримування особи від вчинення протиправного діяння, що створює умови для задоволення інтересів уповноважених суб'єктів владних повноважень і суспільних інтересів в охороні й захисті [91, с. 191-192].

Наведена класифікація правових засобів найбільш повно відображає їх різноманітність та універсальність як регуляторів суспільних відносин. Фактично до правових засобів А. Денисова відносить всі правові явища та процеси, що цілком відповідає реальній дійсності. Штучне створення певного правового явища чи процесу, які не мають на меті досягнення приватних чи публічних цілей правового регулювання, є правовою демагогією або фікцією. Наприклад, прийняття певних декларацій (концепцій, стратегій) про наміри реформування системи цивільного захисту чи про потенціал провадження певних засобів забезпечення безпеки життєдіяльності не призводить до якихось юридично значимих результатів. Результат досягається лише шляхом прийняття конкретного закону чи підзаконного (відомчого) нормативно-правового акту з реальним дієвим інструментарієм реалізації приватних чи публічних інтересів учасників правовідносин.

О. Ганзенко відносить поняття «правові засоби» до ключових категорій інструментальної теорії права. Правові засоби, на його думку, є системою правових форм, методів, способів і прийомів досягнення приватних чи публічних цілей суб'єктами правовідносин. Такий інструментальний підхід до розуміння права дає змогу сприймати його не тільки як сукупність затверджених державою заборон, зобов'язань і дозволів, але й як систему

реальних інструментів задоволення потреб, реалізації інтересів особи, суспільства та держави в цілому [72, с. 36-37].

В цілому така позиція є раціональною, адже інструментальний підхід до поняття та сутності права дозволяє розкрити увесь його потенціал, встановити увесь спектр правових засобів, які можуть бути використані особою для досягнення публічної чи приватної мети правового регулювання.

Таким чином, правові засоби є універсальними засобами правового регулювання, до яких можна віднести і всі інструменти правового впливу органів публічної адміністрації на учасників суспільних відносин.

До правових засобів відносяться і норми права, і принципи права, і способи правового регулювання (заборони, зобов'язання та дозволи), і методи правового регулювання (імперативний, диспозитивний, рекомендаційний), і нормативно-правові акти, і акти тлумачення та застосування норм права, і конклюдентні акти (норми-дії), і нетипові норми права.

Відповідно, правові засоби доцільно класифікувати за різними критеріями:

- за предметом правового регулювання: на конституційні, адміністративні, фінансові, кримінально-правові, цивільно-правові тощо;

- за способом правового регулювання: на правові засоби, які забороняють, зобов'язують та дозволяють;

- за методом правового регулювання: на імперативні, диспозитивні, заохочувальні, рекомендаційні;

- за територією дії: на локальні, загальнодержавні, міждержавні (міжнародні);

- за часом дії: на постійні, тимчасові, разової та періодичної дії;

- за способом психологічного впливу на учасників правовідносин – на обмежуючі та стимулюючі;

- за рівнем конкретизації (за кількістю суб'єктів, на яких вони впливають): на загальні (нормативні), такі, що діють щодо певної групи осіб, та індивідуальні (персональні);

- за рівнем складності – прості та складні (такі, що діють лише у певній сукупності);

- за метою (сферою) правового регулювання: публічно-правові та приватно-правові.

Слід відзначити, що адміністративно-правові засоби як різновид правових засобів, відрізняються особливим порядком застосування, адже суб'єктами, які забезпечують їх практичну реалізацію, є суб'єкти владних повноважень органів публічної адміністрації. Останні діють за спеціально-дозвільним принципом правового регулювання – «дозволено лише те, що прямо передбачено законом». Відповідно, адміністративно-правові засоби мають імперативний (владний) характер та їх дія поширюється, як правило, на територію всієї держави.

Отже, враховуючи наведену класифікацію правових засобів, правові засоби забезпечення безпеки життєдіяльності у більшій частині є адміністративними, постійно діючими на всій території всієї держави, загальними, публічно-правовими, імперативними, такими, що більшою мірою зобов'язують та забороняють, обмежуючими.

Окрему увагу слід приділити правовим засобам забезпечення безпеки життєдіяльності в контексті активної цифровізації процесів публічного управління у вказаній сфері суспільних відносин.

Такими правовими засобами є, зокрема, засоби правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Адміністративно-правове врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності за допомогою адміністративно-правових засобів дозволяє уніфікувати порядок використання інноваційних цифрових інструментів (що в свою чергу забезпечує сумісність програмного забезпечення в процесі взаємодії різних суб'єктів в системі цивільного захисту), а також поширювати позитивний

досвід їх практичної реалізації окремими суб'єктами владних повноважень на територію всієї держави.

Так, наразі детальної адміністративно-правової регламентації потребує порядок застосування інструментарію технології штучного інтелекту, який дозволяє значно оптимізувати процеси публічного управління у сфері забезпечення безпеки життєдіяльності.

До конкретних правових засобів врегулювання питання використання технології штучного інтелекту слід віднести положення розпорядження Кабінету Міністрів України від 9 травня 2025 р. № 457-р., яким затверджено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки [236]. Вказаним Планом, зокрема, передбачено:

- розроблення та подання Кабінетові Міністрів України законопроекту щодо правового врегулювання у сфері розвитку штучного інтелекту (відповідальне – Міністерство цифрової трансформації України);

- розроблення рекомендацій з кібербезпеки, які передбачатимуть пропозиції з використання технологій штучного інтелекту, зокрема щодо захисту моделей машинного навчання від несанкціонованого втручання в роботу (відповідальні – Мінцифри та Адміністрація Держспецзв'язку);

- проведення оцінки стану захищеності інформаційно-комунікаційних систем, які використовують штучний інтелект для виявлення та протидії кіберзагрозам (відповідальна за виконання – Адміністрація Держспецзв'язку);

- застосування технологій штучного інтелекту для проведення державними органами аналізу, прогнозування та моделювання розвитку системи державного управління у відповідних сферах, розрахунок показників ефективності (відповідальні – Мінцифри, Держстат, Мінекономіки, державна установа «Центр обробки статистичних даних», Секретаріат Кабінету Міністрів України);

- забезпечення використання технологій штучного інтелекту у сфері оборони (відповідальні – Міноборони, Апарат Ради національної безпеки і

оборони України, Адміністрація Держспецзв'язку, Фонд розвитку інновацій) [236].

Отже, конкретні правові засоби врегулювання питання використання технології штучного інтелекту передбачають і правову регламентацію використання штучного інтелекту для забезпечення безпеки життєдіяльності, зокрема, кібербезпеки.

Таким чином, перед науковцями та органами публічної адміністрації в Україні стоїть завдання розробити та прийняти відповідний національний закон про штучний інтелект, яким будуть врегульовані всі можливі аспекти використання даної інформаційної технології у різних сферах суспільних відносин, включаючи сферу забезпечення безпеки життєдіяльності. Деталізоване правове регулювання відповідних правовідносин доцільно забезпечити на рівні постанов Кабінету Міністрів України та підзаконних, відомчих нормативно-правових актів.

На окрему увагу заслуговує також питання адміністративно-правового регулювання використання можливостей мобільних застосунків у сфері забезпечення безпеки життєдіяльності.

Так, за допомогою спеціально розробленого мобільного застосунку можна охопити всіх бажаючих приймати участь в ліквідації надзвичайних ситуацій та їх наслідків, тобто потенційних добровольців. Для цього достатньо буде створити базу даних громадян, які через мобільний застосунок нададуть свої анкетні данні, згоду на учать у заходах з ліквідації надзвичайних ситуацій та їх наслідків, а також дані щодо свого місця перебування (доступ до геоданих). Таким чином, мобільний телефон або ноутбук потенційних добровольців буде прив'язаний через спеціальний мобільний застосунок до вказаної бази даних та центру управління, адміністрування якого будуть здійснювати уповноважені посадові особи органу публічної адміністрації, який реалізує державну політику у сфері цивільного захисту. Наразі таким органом публічної адміністрації є Державна служба України з надзвичайних ситуацій.

Отже, у разі виникнення загрози або безпосереднього настання надзвичайної ситуації за допомогою мобільного застосунку зареєстровані в програмі добровольці будуть терміново повідомлятися про можливість долучитися до ліквідації надзвичайної ситуації (пожежі, повені, руйнації об'єктів критичної інфраструктури тощо) та її наслідків. Причому, завдяки геолокації, в першу чергу будуть повідомлятися ті зареєстровані добровольці, які знаходяться поблизу місця виникнення або поширення наслідків надзвичайної ситуації.

В подальшому оператори центру управління вказаним мобільним застосунком зможуть в режимі реального часу координувати діяльність зареєстрованих добровольців, які відгукнулися на виклик та прибули на місце події, надавати поради, отримувати актуальну інформацію з місця події, включаючи трансляцію он-лайн відео, тобто підтримувати постійний двосторонній зв'язок.

Розробка та використання вищевказаного спеціального мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів з метою ліквідації надзвичайних ситуацій та їх наслідків потребує адміністративно-правової регламентації на рівні підзаконного нормативно-правового акту. Так, врегулювати зазначені суспільні відносини доцільно спільним наказом Міністерства внутрішніх справ України та Міністерства цифрової трансформації України, яким необхідно затвердити порядок використання перспективного мобільного застосунку «Я – доброволець».

Вказаним спільним наказом слід визначити права та обов'язки адміністраторів та операторів спеціального мобільного застосунку, а також права та обов'язки добровольців, які зареєструються як потенційні учасники ліквідації надзвичайних ситуацій, порядок та умови забезпечення добровольців спеціальним одягом та спеціальними засобами, а також компенсації транспортних та інших витрат, пов'язаних із прибуттям на місце події.

Також доцільно регламентувати на рівні підзаконних (відомчих) нормативно-правових актів розробку та використання окремого мобільного застосунку для оповіщення населення про загрозу виникнення та безпосередній початок надзвичайної ситуації по аналогії із вже існуючим мобільним застосунком «Повітряна тривога». В сучасних умовах, коли більша частина населення держави є користувачами смартфонів з можливістю використання якісного програмного забезпечення, такий правовий засіб оповіщення населення стане раціональним та зручним доповненням до загальнодержавної системи оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій, яка передбачена Положенням про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, затвердженим постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733 [250].

Таким чином, інструментальний підхід (теорія правових засобів) дозволяє ефективно виявити актуальні проблеми адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та сформулювати конкретні пропозиції щодо удосконалення чинного національного законодавства та юридичної практики у даній сфері суспільних відносин.

На окрему увагу заслуговує питання реалізації публічних та приватних інтересів в процесі адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Будь-які суспільні відносини обумовленні певними інтересами їх учасників. В залежності від спрямованості інтереси поділяються на публічні та приватні. Інтереси виникають із природних та інших потреб людини та необхідності реалізації та захисту загальних потреб всього суспільства. До останніх слід віднести: необхідність забезпечення законності та правопорядку, що є умовою безпечної життєдіяльності кожного члена суспільства; необхідність розвитку економіки, засобів виробництва, що є умовою

підвищення рівня життя (реального доходу на душу населення); необхідність захисту навколишнього природного середовища, що є умовою безпечного функціонування в ньому кожного окремого індивіда; необхідність забезпечення національної безпеки та оборони від зовнішньої збройної агресії та внутрішніх деструктивних процесів; інші потреби, які забезпечують нормальне функціонування та розвиток суспільства.

Враховуючи загальне значення та важливість публічних інтересів, вони як правило закріплені в нормах Конституції та законів, санкціоновані державою, тобто їх реалізація та захист забезпечується органами публічної адміністрації, а за порушення передбачена цивільно-правова, адміністративна або кримінальна відповідальність. Так, наприклад, однією із функцій органів прокуратури є представництво інтересів держави в суді у виключних випадках і в порядку, що визначені законом.

Одним із публічних інтересів, який відображений в нормах чинного національного законодавства, є забезпечення безпеки життєдіяльності, що включає в себе і систему цивільного захисту населення та територій від надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру.

Окремий публічний інтерес становить використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, адже інформаційні технології дозволяють значно оптимізувати сили та засоби забезпечення життєдіяльності та цивільного захисту.

Водночас використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності обумовлено і приватним інтересом – отримати необхідну інформацію про стан забезпечення безпеки життєдіяльності, доступні інструменти цивільного захисту та порядок їх використання, долучитися до ліквідації надзвичайної ситуації та її наслідків тощо.

Таким чином, дослідження особливостей реалізації публічних та приватних інтересів в процесі адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки

життєдіяльності має як теоретичне, так і практичне значення для формулювання пропозицій щодо удосконалення чинного законодавства у даній сфері суспільних відносин.

Публічні та приватні інтереси присутні у всіх суспільних відносинах, адже будь-яка галузь права покликана забезпечувати реалізацію як інтересів суспільства в цілому, так і інтересів кожної окремої людини.

В адміністративному праві, яке відноситься до галузей публічного права, більшою мірою регламентовано реалізацію та захист саме публічних інтересів, адже його норми регулюють відносини публічного управління та адміністрування суспільних відносин, відносини між людиною та органами публічної адміністрації.

О. Бака зазначає, що з точки зору адміністративно-правової науки, публічний інтерес – це інтерес соціальної спільності, що визнаний та задоволений державою. Визнання публічності інтересу здійснюється шляхом його правового (юридичного) забезпечення (фіксації в нормах і встановленні механізму реалізації) [16, с. 151].

Також О. Бака справедливо зауважує, що оскільки публічними є суспільні інтереси, які забезпечуються та охороняються державою, держава здійснює заходи з реалізації публічного інтересу безпосередньо або встановленням нормативних приписів, обмежень, заборон, які регламентують діяльність суб’єктів права [16, с. 152].

Оптимальне співвідношення публічних і приватних інтересів як у соціальній практиці, так і в правовому регулюванні, на його думку, є необхідною умовою гармонійного розвитку суспільства, окремої особистості, ефективності функціонування держави [16, с. 153].

Отже, в процесі здійснення правового регулювання суспільних відносин важливим є забезпечення діалектики публічних та приватних інтересів, які з одного боку часто є протилежними, а з іншого – об’єднуються єдиною метою правового регулювання – забезпечити належне впорядкування суспільних відносин, що виражається в дотриманні режиму законності та забезпеченні

стану правопорядку з метою нормального функціонування та розвитку суспільства та кожного окремого індивіда.

У сфері забезпечення безпеки життєдіяльності публічний інтерес безумовно посідає ключове місце, адже відповідна наука та навчальна дисципліна створені з метою інформування людей про різні види небезпек та засоби захисту від них. Водночас приватні інтереси полягають у бажанні кожного захистити своє життя та здоров'я від негативних факторів навколишнього природного середовища, техногенних негативних факторів, наслідків соціальних конфліктів та загроз воєнного характеру.

Співвідношення публічних та приватних інтересів відображено, зокрема, у визначенні поняття безпеки життєдіяльності. Так, науковці зазначають, що безпека життєдіяльності – це наука, що вивчає проблеми безпечного перебування людини в середовищі – природному, техногенному, соціальному, в процесі різних видів її діяльності. Вона, на їх думку, є більш універсальною, ніж окремі напрямки наукових досліджень, такі як охорона праці чи цивільний захист, адже дві останні розглядають лише окремі випадки безпеки в конкретних ситуаціях, зокрема охорона праці вивчає питання безпеки людини, яка знаходиться в умовах виробництва, а цивільний захист – в надзвичайних ситуаціях, тоді як безпека життєдіяльності – у всіх життєвих обставинах [16, с. 8].

Таким чином, у сфері забезпечення цивільного захисту публічний інтерес є домінуючим, адже головним завданням цивільного захисту є захист населення (тобто суспільства в цілому) та територій від надзвичайних ситуацій природного, техногенного, соціального та воєнного характеру.

Так, у відповідності до ст. 4 Кодексу цивільного захисту України, цивільний захист – це комплекс заходів, які реалізуються на території України в мирний час та в особливий період і спрямовані на захист населення, територій, навколишнього природного середовища, майна, матеріальних і культурних цінностей від надзвичайних ситуацій та інших небезпечних подій, запобігання виникненню таких ситуацій та подій, ліквідацію їх наслідків,

надання допомоги постраждалим, здійснення державного нагляду (контролю) у сфері пожежної та техногенної безпеки [143].

Водночас безпека життєдіяльності, як зазначає О. Арламов, це галузь знання та науково-практична діяльність, спрямована на вивчення загальних закономірностей виникнення небезпек, їхніх властивостей, наслідків їхнього впливу на організм людини, основ захисту здоров'я та життя людини і середовища її проживання від небезпек, а також на розробку і реалізацію відповідних засобів та заходів щодо створення і підтримки здорових та безпечних умов життя і діяльності людини як у повсякденних умовах побуту та виробництва, так і в умовах надзвичайних ситуацій [12, с. 3].

Отже, публічний інтерес у сфері безпеки життєдіяльності полягає у забезпеченні безпечного середовища для життя та розвитку кожної людини та суспільства в цілому.

Натомість публічний інтерес у сфері цивільного захисту полягає в забезпеченні оперативної ліквідації надзвичайних ситуацій та їх наслідків.

Найбільш повно публічний інтерес у сфері цивільного захисту відображено у ст. 1 Кодексу цивільного захисту України, в якій, зокрема, зазначено, що кодекс 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, 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 [143].

До законів, які відображають публічний інтерес у здійсненні адміністративно-правового регулювання у сфері забезпечення безпеки

життєдіяльності, слід віднести закони України «Про правовий режим надзвичайного стану» [273], «Про дорожній рух» [234], «Про основні принципи та вимоги до безпечності та якості харчових продуктів» [270], «Про охорону праці» [271] та інші закони, які так чи інакше стосуються питань забезпечення безпеки життєдіяльності.

Публічний інтерес реалізується також в процесі адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності шляхом досягнення конкретної мети публічного управління – впорядкування відповідних суспільних відносин з використанням цифрових технологій у відповідності до принципу належного урядування, що забезпечує оперативне реагування на надзвичайні ситуації, швидку мобілізацію матеріально-технічних та людських ресурсів для ліквідації надзвичайної ситуації та її наслідків, попередження виникнення аналогічних надзвичайних ситуацій у майбутньому.

Значною мірою удосконалення механізмів реагування на надзвичайні ситуації відбувається саме завдяки впровадженню нових інформаційних технологій, до яких слід віднести автоматизовані інформаційні системи, використання мобільних застосунків, технології штучного інтелекту тощо.

Публічний інтерес також чітко простежується у функціях та повноваженнях Міністерства цифрової трансформації України, яке координує діяльність інших органів публічної адміністрації у сфері впровадження та використання інформаційних технології (цифровізації). Так, згідно із Положенням про Міністерство цифрової трансформації України, затвердженим 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 сфері надання електронних та адміністративних послуг; у сфері хмарних послуг; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів, електронних комунікацій, розвитку інфраструктури широкосмугового доступу до Інтернету, електронної комерції та бізнесу; у сферах електронної ідентифікації та електронних довірчих послуг; у сфері розвитку IT-індустрії; у сфері розвитку та функціонування правового режиму Дія Сіті [222].

Таким чином, адміністративно-правова регламентація використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності повинна здійснюватися за участю Міністерства цифрової трансформації України з метою оптимальної реалізації публічних та приватних інтересів в процесі правового регулювання відповідних суспільних відносин. Отже, основні засади та порядок використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності доцільно затверджувати спільними наказами МВС України та Міністерства цифрової трансформації України. Тільки спільна нормотворчість вказаних органів публічної адміністрації забезпечить реалізацію ключових публічних інтересів у даній сфері суспільних відносин.

Адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності покликано забезпечити єдиний, стандартизований підхід до використання відповідного ліцензованого актуального програмного забезпечення для автоматизації систем забезпечення безпеки життєдіяльності та цивільного захисту, тобто сумісність цифрових продуктів, які використовуються різними органами публічної адміністрації. Крім того, адміністративно-правове регулювання вказаних суспільних відносин дозволяє забезпечити належний рівень захисту інформаційних ресурсів шляхом їх централізованого криптографічного шифрування та зберігання на кількох автономних (альтернативних) серверах, а також дозволяє оперативно поширювати локальний позитивний досвід

використання певного програмного забезпечення, окремих технічних засобів та технологій на територію всієї держави.

Яскравим прикладом забезпечення оптимального співвідношення публічних та приватних інтересів в процесі адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності є розробка та правова регламентація використання перспективного мобільного застосунку «Я-доброволець».

Так, у Львівському державному університеті безпеки життєдіяльності відбулося виїзне засідання Комітету Верховної Ради України з питань екологічної політики та природокористування на тему: «Про стан функціонування добровільної та місцевої пожежної охорони» [349].

В рамках засідання було проведено семінар-нараду з питань розвитку підрозділів добровільної та місцевої пожежної охорони.

На засіданні серед іншого було обговорено вдосконалення законодавчої бази у сфері організації та функціонування місцевої та добровільної пожежної охорони. Одним із питань порядку денного було представлення концепції системи оповіщення та реагування «Я – доброволець». Під час дискусії учасники обговорили основні етапи розробки системи, можливі варіанти її архітектури, способи залучення членів добровільних формувань до системи. За результатами наради було погоджено план подальшої співпраці в рамках реалізації системи оповіщення та реагування «Я – доброволець» [349].

Ідея цієї системи полягає у створенні інноваційної платформи для організації та координування дій соціально активних громадян, які готові долучитись до ліквідації наслідків надзвичайних подій відповідно до свого фаху. Це вкрай важлива та необхідна на сьогодні ініціатива, що вже давно функціонує у зарубіжних країнах [349].

Таким чином, система оповіщення та реагування «Я – доброволець» потребує належної адміністративно-правової регламентації та впровадження в практичну діяльність з використанням відповідного мобільного застосунку.

Так, в Хмельницькій ОВА 15 серпня 2024 року відбулася презентація напрацьованої програми і постановка нових завдань для тестового впровадження системи «Я-Доброволець» в Головних управліннях ДСНС України у Львівській та Хмельницькій областях [296].

Як зауважив голова Хмельницької ОВА Сергій Тюрін, система оповіщення та реагування «Я-Доброволець» – це інноваційна платформа, що дозволить організувати та координувати дії соціально активних громадян, які готові долучитися до ліквідації наслідків надзвичайних подій, використовуючи свій професійний досвід і навички. Тобто, завдяки додатку для смартфона, кожен охочий може стати на захист своєї громади, отримуючи вказівки та інструкції щодо подолання небезпек. Така платформа також дозволить вносити всі необхідні відомості про добровольця до інформаційної бази, аби оперативно та своєчасно повідомляти людину про її можливе залучення до ліквідації надзвичайних ситуацій [296].

Сергій Тюрін також справедливо наголосив на тому, що «реалізація Системи оповіщення та реагування «Я-Доброволець» на території області не лише допоможе швидко реагувати на будь-які надзвичайні ситуації, але й впровадити європейський досвід у регіоні. Це стане новим кроком до підвищення безпеки та соціальної відповідальності громадян» [296].

Таким чином, поширення позитивного досвіду використання Системи оповіщення та реагування «Я-Доброволець» та відповідного мобільного застосунку на територію всієї держави дозволить реалізувати як публічні так і приватні інтереси учасників відповідних суспільних відносин. Так, кожен громадянин зможе реалізувати свій приватний інтерес у формі бажання прийняти особисту участь в ліквідації надзвичайної ситуації та її наслідків (проявити соціальну активність та отримати відповідний досвід роботи рятувальником). Водночас збільшення кількості потенційних добровольців та активне використання вказаного мобільного застосунку з урахуванням геолокації (місцезнаходження) користувачів дозволить забезпечити публічний

інтерес – оперативно мобілізувати людські та матеріально-технічні ресурси для ліквідації надзвичайних ситуацій.

Отже, публічний інтерес у сфері безпеки життєдіяльності полягає у забезпеченні безпечного середовища для життєдіяльності та розвитку суспільства. Натомість публічний інтерес у сфері цивільного захисту полягає в забезпеченні оперативної ліквідації надзвичайних ситуацій та їх наслідків.

Водночас, не зважаючи на публічно-правовий характер суспільних відносин, які врегульовані Кодексом цивільного захисту України та законами України у сфері забезпечення безпеки життєдіяльності, приватні інтереси відіграють ключову роль в процесі адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. Зокрема, нормативно регламентоване впровадження інформаційних технологій у сфери забезпечення безпеки життєдіяльності та цивільного захисту дозволяє реалізувати наступні приватні інтереси учасників відповідних суспільних відносин: доступ кожного до відкритих публічних баз даних про місця виникнення та локалізації наслідків надзвичайних подій та ситуацій; загальний доступ до інтерактивних карт захисних споруд, укриттів з урахуванням геолокації особи, яка шукає захист (наприклад, чат-бот «Укриття»); можливість використання перспективного мобільного застосунку «Я доброволець», який дозволяє кожному долучитися до ліквідації надзвичайних ситуацій та їх наслідків.

Адміністративно-правова регламентація та поширення позитивного досвіду використання Системи оповіщення та реагування «Я-Доброволець» та відповідного мобільного застосунку на територію всієї держави дозволить реалізувати як приватні інтереси у формі реальних потреб громадян у соціальній активності та можливості прийняти особисту участь в ліквідації надзвичайних ситуацій та їх наслідків, так і публічні інтереси у формі суспільної потреби в мобілізації людських ресурсів для ліквідації конкретної надзвичайної ситуації та навчання громадян основам рятувальної справи та тактиці аварійно-рятувальних робіт.

4.3 Перспективні напрями удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту

Сучасне цифровізоване суспільство розвивається в складних кліматичних умовах, пов'язаних із глобальним потеплінням. Крім того, значну загрозу безпеці життєдіяльності цивілізованих країн несуть загрози воєнного характеру, пов'язані із збройною агресією сусідніх держав. Для України, яка потерпає від повномасштабного вторгнення російської федерації актуальними також є загрози техногенного та соціального характеру, адже об'єктами цілеспрямованих ракетних обстрілів з боку росії є національна енергетика та критична інфраструктура, а об'єктом інформаційних атак та дезінформації є українське суспільство.

Таким чином, органам публічної адміністрації в Україні необхідно подвоювати зусилля щодо належного забезпечення безпеки життєдіяльності населення та запобігання виникненню надзвичайних ситуацій техногенного, природного, соціального та воєнного характеру.

Ключовим інструментом оптимізації публічного управління у сферах цивільного захисту та забезпечення безпеки життєдіяльності є цифровізація, тобто використання інноваційних інформаційних технологій для мобілізації людських та матеріально-технічних ресурсів з метою ліквідації надзвичайних ситуацій та їх наслідків. До інноваційних цифрових інструментів слід віднести інформаційно-телекомунікаційні системи, автоматизовані та роботизовані системи, мобільні застосунки та інше програмне забезпечення, а також технологію штучного інтелекту.

Враховуючи спеціально-дозвільний принцип, якого повинні дотримуватися в своїй діяльності органи публічної адміністрації, використання інноваційних інформаційних технологій в процесі здійснення публічного управління (адміністрування суспільних відносин) потребує чіткої адміністративно-правової регламентації.

Враховуючи вищевикладене, дослідження актуальних напрямів удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності має як теоретичне, так і практичне значення.

Як вже було зазначено у попередніх розділах роботи, основним нормативно-правовим актом, який регулює суспільні відносини у сфері цивільного захисту та у сфері забезпечення безпеки життєдіяльності в цілому є Кодекс цивільного захисту України. Так, вказаний кодекс 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 [143].

Таким чином, Кодексом цивільного захисту України передбачено функціонування єдиної державної системи цивільного захисту, більш детальна правова регламентація функціонування якої здійснена на рівні Положення про єдину державну систему цивільного захисту, затвердженого постановою Кабінету Міністрів України від 9 січня 2014 р. № 11 [249].

Так, у відповідності до вказаного Положення, єдина державна система цивільного захисту – це сукупність органів управління, сил і засобів центральних та місцевих органів виконавчої влади, виконавчих органів рад, підприємств, установ та організацій, які забезпечують реалізацію державної політики у сфері цивільного захисту. Органами управління цивільного захисту згідно із зазначеним Положенням є органи виконавчої влади, виконавчі органи міських, районних у містах (у разі їх створення), селищних та сільських рад, керівні органи підприємств, установ та організацій, а також їх структурні підрозділи (посадові особи), призначені для безпосереднього керівництва діяльністю у сфері цивільного захисту відповідно до компетенції.

Положенням про єдину державну систему цивільного захисту також передбачено, що керівництво єдиною державною системою цивільного захисту здійснює Кабінет Міністрів України, проте безпосереднє керівництво

діяльністю єдиної державної системи цивільного захисту здійснює ДСНС України [249].

Пунктами 6-8 вказаного Положення передбачено, що єдина державна система цивільного захисту складається з постійно діючих функціональних і територіальних підсистем. Функціональні підсистеми єдиної державної системи цивільного захисту створюються у відповідних сферах суспільного життя центральними органами виконавчої влади з метою захисту населення і об'єктів функціональної підсистеми від надзвичайних ситуацій у мирний час та в особливий період, здійснення заходів цивільного захисту відповідного галузевого спрямування, забезпечення готовності підпорядкованих їм сил і засобів до дій, спрямованих на запобігання і реагування на надзвичайні ситуації. Безпосереднє керівництво діяльністю функціональної підсистеми здійснюється керівником органу чи суб'єкта господарювання, що створив таку підсистему [249].

Територіальні підсистеми єдиної державної системи цивільного захисту створюються з метою здійснення заходів щодо захисту населення і територій від надзвичайних ситуацій у мирний час та в особливий період у відповідному регіоні.

У складі єдиної державної системи цивільного захисту функціонують постійно діючі органи управління цивільного захисту, координаційні органи, сили цивільного захисту функціональних і територіальних підсистем (п. 9 вказаного Положення) [249].

Позитивно оцінюючи наведену структуру національної системи цивільного захисту, слід відзначити, що сучасні інформаційні технології дозволяють суттєво оптимізувати процеси публічного управління єдиною державною системою цивільного захисту.

Так, на даний час «Система управління силами та засобами цивільного захисту» є підсистемою єдиної інформаційної системи Міністерства внутрішніх справ. Згідно із Положенням про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної

інформаційної системи Міністерства внутрішніх справ, затвердженим наказом Міністерства внутрішніх справ України від 20.04.2023 № 326, СУСЗ (система управління силами та засобами цивільного захисту) – це інтегрована інформаційно-комунікаційна система, що забезпечує збирання, зберігання, використання, передачу, захист інформації про сили та засоби цивільного захисту, об’єкти, на яких існує загроза виникнення надзвичайних ситуацій, пожеж та інших небезпечних подій, у тому числі об’єкти підвищеної небезпеки, надзвичайні ситуації, небезпечні події, у тому числі пожежі, а також іншої інформації, необхідної для керування силами та засобами цивільного захисту, а також оперативно-диспетчерського управління ними [255].

Проте вказана «Система управління силами та засобами цивільного захисту» фактично є відомчою інформаційно-комунікаційною системою, а саме – підсистемою єдиної інформаційної системи Міністерства внутрішніх справ України. Враховуючи важливість ефективної організації управління силами та засобами цивільного захисту в умовах воєнного стану, вказана система повинна бути самостійним та самодостатнім цифровим продуктом, який буде адмініструвати ДСНС України.

Також потребує удосконалення Інформаційна система «Облік та візуалізація фонду захисних споруд цивільного захисту», яка розміщена на офіційному сайті Державної служби України з надзвичайних ситуацій. Завдяки підтримці Міністерства цифрової трансформації України система обліку укриттів доступна в застосунку «Дія».

Проте, з точки зору користувача вказана інформаційна система не має достатнього інтерфейсу для ефективного використання. Зокрема, доцільно додати до неї можливість прокласти маршрут слідування особи від точки її місцезнаходження до найближчого укриття за допомогою інструменту визначення геолокації, тобто додати до інтерактивної мапи функції навігатора.

Таким чином, враховуючи зростаючі загрози природнього, техногенного, соціального та воєнного характеру, одним із напрямів

удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності є створення єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати, серед іншого, інтерактивну мапу захисних укриттів, місць локалізації надзвичайних ситуацій та їх наслідків (за виключенням місць прильотів ворожих ракет та безпілотних літальних апаратів), а також інформаційну базу суб'єктів забезпечення цивільного захисту.

Адміністративно-правова регламентація створення єдиної інформаційно-телекомунікаційної системи цивільного захисту буде сприяти подальшому впровадженню інформаційних технологій в діяльність Державної служби України з надзвичайних ситуацій.

У зв'язку із цим І. Подобєд слушно зазначає, що цифрова трансформація ресурсного механізму висуває на порядок денний питання реформування державного управління у сфері цивільного захисту. В умовах сучасного стану, з одного боку, обсяги і зміст завдань, які постають перед системою цивільного захисту, зростають та ускладнюються, а з іншого – алгоритми роботи, що існують, потребують удосконалення. Цифровізація торкнулася практично всіх сфер роботи цієї системи, від внутрішніх комунікацій і планування ресурсів до оцінки ситуації. Незважаючи на те, що останніми роками ресурсний механізм сфери цивільного захисту покращив свою здатність краще адаптуватися до потенціалу нових технологічних розробок, все ще є місце для вдосконалення. Більша ясність у законодавстві та нормативних актах допоможе органам цивільного захисту оцінити, як нові технології можна використовувати на практиці. Відповідне законодавство та регулювання також дадуть можливість усунути ризики та виклики, що пов'язані із застосуванням нових технологій [216, с.98].

Особливої актуальності питання цифровізації діяльності ДСНС України набуває в умовах дії правового режиму воєнного стану.

Так, згідно із підсумками 2022 року щодо цифровізації ДСНС України,

які розміщені на офіційному веб-сайт служби, ключовим завданням органу публічної адміністрації, який реалізує державну політику у сфері цивільного захисту, було підвищення внутрішньої ефективності роботи в умовах війни та створення ряду сервісів, які б допомагали вчасно інформувати населення про загрози та зберегти життя і здоров'я українців. Один з таких сервісів – це сервіс протимінної діяльності ДСНС. Зважаючи на величезне забруднення території України вибухонебезпечними предметами, ДСНС за підтримки партнерів створило Сервіс, доступний у веб версії та в додатках, який дає змогу повідомити про знахідку ВНП (вибухонебезпечних предметів), попередити про небезпечні території, а також має чітку інструкцію, як поводитись при подібній знахідці. Протягом 2022 року до ДСНС України надійшло близько 17 тисяч повідомлень про знахідку потенційних вибухонебезпечних предметів, з яких близько 1000 заявок саме через вказаний Сервіс [211].

Крім того, у 2022му році було оновлено офіційний веб-сайт ДСНС України. Відбулось, зокрема, наповнення його актуальною інформацію щодо ситуації в умовах війни. Також було створено інформаційний чат-бот служби у WhatsApp. У Telegram створений чат-бот «Інтерактивний інспектор» з метою надання інформаційної підтримки суб'єктам господарювання, що дозволяє обрати тип та необхідну кількість вогнегасників, визначити клас зони приміщення залежно від параметрів його функціонування.

Також було продовжено модернізацію «Порталу електронних послуг ДСНС» через який можна подати декларацію відповідності матеріально-технічної бази суб'єкта господарювання вимогам законодавства з питань пожежної безпеки, або отримати ліцензію на провадження господарської діяльності з надання послуг і виконання робіт протипожежного призначення всього за декілька хвилин, маючи електронний підпис [211].

Крім того, згідно з підсумки 2022 року в напрямі цифровізації, ДСНС України спільно з мобільними операторами розгорнула сучасну систему інформування населення «Cell Broadcast», яка інтегрована у загальнодержавну

систему оповіщення населення про надзвичайні події для використання місцевими органами виконавчої влади. Відповідне обладнання загальнодержавної системи оповіщення було закуплене, передане і розгорнуте у військово-цивільних адміністраціях України.

Також ДСНС України розпочала масштабний проєкт перебудови системи радіозв'язку з аналогового на сучасний цифровий, і незважаючи на величезний ресурс, який необхідний для цього, завдяки підтримці МВС та Уряду України було переведено на цифровий радіозв'язок 4 регіони [211].

Крім того, у 2022му році було продовжено модернізацію Оперативно-координаційних центрів в Головних управліннях ДСНС України, які під час війни відіграють одну з ключових ролей в координації системи реагування на надзвичайні ситуації. За 2022 рік було модернізовано 8 центрів, в яких не лише встановлене сучасне обладнання та створені комфортні умови роботи операторів, але й впроваджується інноваційна система управління силами та засобами, яка спрямована на автоматизацію направлення підрозділів ДСНС на місце надзвичайної ситуації.

Значний ресурс був спрямований на комплексне оновлення парку комп'ютерної техніки служби, а також завершено впровадження системи електронного документообігу в ДСНС до рівня районів [211].

Окрему увагу було приділено повній перебудові архітектури зберігання та обробки даних на серверних потужностях в ДСНС. Заплановано провадження сучасної логістичної системи для ефективного та прозорого управління майном ДСНС, повний перехід на електронні системи фінансового та кадрового обліку, впровадження системи енергоменеджменту, створення ряду реєстрів, на виконання вимог закону щодо переходу на систему страхування пожежної безпеки [211].

Таким чином, незважаючи на надскладні умови роботи в умовах воєнного стану, ДСНС України здійснює активні заходи щодо впровадження інноваційних інформаційних технологій у сферу забезпечення безпеки життєдіяльності та цивільного захисту.

Слід відзначити, що процеси цифровізації діяльності Державної служби України з надзвичайних ситуацій відображені також у Звіті про основні результати діяльності служби.

Так, у відповідності до Звіту про основні результати діяльності Державної служби України з надзвичайних ситуацій у 2023 році, 07 жовтня 2023 року запроваджено Державний електронний реєстр об'єктів підвищеної небезпеки, яким унормовано спрощену та прозору процедуру опрацювання матеріалів ідентифікації об'єктів (понад 5 тис. матеріалів).

Забезпечено доступ працівників ДСНС до роботи в електронному кабінеті посадової особи ДСНС у Єдиній державній електронній системі у сфері будівництва.

Діджиталізовано перевірку професійних знань рятувальників, які підлягають атестації у Міжвідомчій комісії з атестації аварійно-рятувальних служб і рятувальників [118].

Крім того, у відповідності до вказаного Звіту, запроваджено спрощену процедуру подання декларації відповідності матеріально-технічної бази суб'єкта господарювання вимогам законодавства з питань пожежної безпеки через смартфон та Єдиний портал державних послуг «Дія». Презентовано новий комплексний сервіс «е-Підприємець».

Також здійснювалась робота щодо впровадження Реєстру організацій, що проводять аудит пожежної та техногенної безпеки, та експертів у сфері пожежної та техногенної безпеки та Реєстру договорів страхування відповідальності за шкоду, яка може бути заподіяна третім особам внаслідок надзвичайних ситуацій, небезпечних подій, у тому числі пожеж та аварій на території та/або об'єктах нерухомості [118].

До позитивних результатів впровадження інформаційних технологій в діяльність ДСНС Україні слід віднести створення чат-боту «ДСНС» на платформі WhatsApp for Business від Turn.io, завдяки якому користувачі мають змогу отримувати достовірну інформацію та корисний контент: що робити у надзвичайній ситуації, як надавати домедичну допомогу, як діяти під час

обстрілів тощо.

Також слід відзначити створення чат-боту «Інтерактивний інспектор» на платформі Telegram, завдяки якому громадяни, керівники підприємств, суб'єкти господарювання можуть отримати швидко та автоматично консультації щодо забезпечення пожежної безпеки своїх об'єктів. Функціонал чат-бота постійно розширюється [118].

Проте, платформа Telegram має російські коріння та становить потенційну загрозу інформаційній безпеці України, адже активно використовується спеціальними службами російської федерації.

Так, в Україні за рішенням РНБО співробітникам органів публічної адміністрації та військовослужбовцям заборонили користуватися Telegram. Радою національної безпеки та оборони України зокрема було прийнято рішення щодо заборони встановлення та використання Telegram на службових пристроях працівників органів державної влади, військовослужбовців, працівників сектору безпеки і оборони, а також підприємств – операторів критичної інфраструктури [229].

Крім того, відбулося засідання Національного координаційного центру кібербезпеки (НКЦК), який є ключовим органом координації та контролю у сфері кібербезпеки. У вказаному засіданні взяли участь представники керівного складу Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Генерального штабу Збройних Сил України, Міністерства оборони України, Національної поліції України, Національного банку України, Міністерства цифрової трансформації України, Міністерства закордонних справ України, розвідувальних органів, керівництво регуляторних органів у сфері електронних комунікацій, а також народні депутати України.

Представники СБУ та Генерального штабу ЗСУ зазначили, що Telegram активно використовується ворогом для кібератак, розповсюдження фішингу та шкідливого програмного забезпечення, встановлення геолокації користувачів, корегування ракетних ударів тощо [229].

Також слід відзначити, що Telegram активно використовується спецслужбами російської федерації для вербовки громадян України з метою проведення ними підривної діяльності, вчинення терактів та збору інформації про переміщення сил та засобів Збройних Сил України.

Враховуючи описані загрози, в контексті необхідності забезпечення безпеки життєдіяльності громадян України та запобігання надзвичайним ситуаціям (причиною яких є диверсійна діяльність завербованих через Telegram осіб), мобільний застосунок Telegram доцільно взагалі заборонити до використання в Україні та блокувати доступ до нього для населення.

Отже, на окрему увагу заслуговує питання удосконалення адміністративно-правового регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності.

Сучасна система цивільного захисту функціонує в складних умовах правового режиму воєнного стану, коли рятувальники задіяні в ліквідації надзвичайних ситуацій воєнного характеру, спричинених масованими артилерійськими обстрілами, ракетно-бомбовими атаками проти цивільної та критичної інфраструктури України. Також актуалізувалась потреба термінового сповіщення громадян про ворожі обстріли з метою проведення евакуації в захисні укриття. Стара система оповіщення з використанням засобів радіомовлення та телебачення є неефективною, а сирена повітряної тривоги, яка поширюється гучномовцями, є неінформативною. На допомогу в цій ситуації прийшли мобільні застосунки, яскравим прикладом яких є мобільний застосунок «Повітряна тривога», який дозволяє стежити за початком та відбоєм сирен у певному регіоні та країні в цілому. Не менш позитивним прикладом є чат-бот «Укриття», який дозволяє користувачу знайти найближчу захисну споруду з урахуванням його місцезнаходження (геолокації).

Проте потенціал мобільних застосунків та іншого програмного забезпечення, в контексті можливості їх використання у сфері забезпечення

безпеки життєдіяльності, наразі не вичерпано, адже існує значна кількість актуальних питань у даній сфері суспільних відносин, які потребують оперативного вирішення за допомогою інноваційних інформаційних технологій. Серед них: потреба оперативної мобілізації людських та матеріально-технічних ресурсів для ліквідації надзвичайних ситуацій та їх наслідків, питання організації взаємодії підрозділів ДСНС України та добровольців, які приймають участь в ліквідації надзвичайної ситуації.

Сучасні інформаційні технології дозволяють суттєво покращити життя людей, зокрема, забезпечити швидкий доступ до будь-якої публічної інформації, організувати комунікацію (зв'язок) незалежно від відстаней та кількості учасників спілкування, удосконалити сфери виробництва та надання послуг шляхом їх автоматизації, розширити можливості людини у сфері освіти, медицини, культури тощо.

У сфері публічного управління інформаційні технології дозволяють спростити бюрократичні процедури отримання адміністративних послуг, перейти на електронний документообіг, суттєво покращити двосторонній зв'язок між органами публічної адміністрації та фізичними і юридичними особами, надати суб'єктам владних повноважень зручний інструментарій електронного урядування для здійснення публічного управління та адміністрування суспільних відносин (швидка ідентифікації особи, цифровий підпис, оперативний обмін службовою інформацією та ефективний контроль виконання поставлених завдань).

Одним із найбільш поширених видів використання інформаційних технологій у повсякденному житті є мобільні застосунки.

Мобільний застосунок є різновидом програмного забезпечення, яке використовується для роботи на портативних пристроях, до яких відносять смартфони, планшети, смарт-годинники.

Мобільні застосунки дозволяють пов'язати портативний пристрій (гаджет) певної особи із певною інформаційною системою та додати до можливостей портативного пристрою нові функції – обробляти певним чином

інформаційні ресурси (систематизувати, виділяти фрагменти та встановленими алгоритмами), записувати та редагувати фото та відеофайли, надсилати повідомлення та підтримувати комунікацію (інформаційний зв'язок) із іншими користувачами відповідного програмного забезпечення тощо.

Мобільні застосунки дозволяють значною мірою оптимізувати роботу корпоративних інформаційних систем, покращити механізм публічного управління та адміністрування суспільних відносин в цілому.

Водночас в умовах триваючої повномасштабної збройної агресії російської федерації проти України особливої актуальності набули питання удосконалення системи цивільного захисту громадян та суспільства в цілому від надзвичайних ситуацій воєнного характеру.

Так, одним із перших завдань цивільного захисту в умовах правового режиму воєнного стану є своєчасне оповіщення громадян про загрозу ворожого обстрілу. На допомогу вже існуючим засобам оповіщення громадян, що передбачені Положенням про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, яке затверджене постановою Кабінету Міністрів України від 27 вересня 2017 року № 733 [250], прийшли можливості мобільних застосунків, тобто спеціального програмного забезпечення, яке встановлюється на смартфон чи персональних комп'ютер.

Так, компанією Ajax System за підтримки Міністерства цифрової трансформації України був розроблений мобільний застосунок «Повітряна тривога», який дозволяє стежити за початком та відбоєм сирен у певному регіоні та країні в цілому.

Мобільний застосунок «Повітряна тривога» інформує користувача про початок і завершення повітряних, техногенних, хімічних, та інших тривог єдиної державної системи цивільного захисту (цивільної оборони). Причому вказаний мобільний застосунок надсилає користувачу звукові та візуальні сигнали про початок тривоги, навіть коли смартфон знаходиться у сплячому

або беззвучному або режимі. Крім того, мобільний застосунок «Повітряна тривога» є безкоштовним та не вимагає від користувача надання персональних даних.

Крім того, компанія Stfalcon за підтримки ДСНС України створила чат-бот Укриття! @UkraineShelterStfalconBot, який дозволяє користувачу знайти найближчу захисну споруду з урахуванням його місцезнаходження (геолокації). Проте цей чат-бот не належить органам публічної адміністрації, тому персональні дані, які надає особа, фактично не захищені. Водночас цей чат-бот може збирати дані про геолокацію (місцезнаходження) особи, її номер телефону. Тому цьому та подібним сервісам не можна довіряти реквізити офіційних документів, логіни та паролі входу до аккаунтів користувача тощо.

Враховуючи те, що переважна кількість громадян є користувачами смартфонів, мобільні застосунки є зручним та універсальним допоміжним інструментом інформування громадян про загрозу виникнення або виникнення надзвичайних ситуацій.

Як видно із вищезазначеного розробниками вказаних мобільних застосунків є комерційні та волонтерські організації, ІТ-компанії, тому вони не потребують правової регламентації.

Сучасні інформаційні технології дозволяють також оперативно мобілізувати людські та матеріально-технічні ресурси для виконання актуальних завдань цивільного захисту. Так, за допомогою спеціального мобільного застосунку можливо швидко поінформувати його користувачів про місце та час виникнення надзвичайної ситуації, її характер та необхідні сили та засоби для її ліквідації, а також координувати дії осіб, які зголосилися прийняти участь в рятувальних роботах.

Прикладом такого спеціального мобільного застосунку є перспективна система оповіщення та реагування «Я – доброволець».

Ідея цієї системи полягає у створенні інноваційної платформи для організації та координування дій соціально активних громадян, які готові долучитись до ліквідації наслідків надзвичайних подій відповідно до свого

фаху. Це вкрай важлива та необхідна на сьогодні ініціатива, що вже давно функціонує у зарубіжних країнах [349].

Для приєднання до системи оповіщення та реагування «Я – доброволець» кожен бажаючий зможе завантажити відповідний мобільний застосунок та надати свої персональні дані і добровільну згоду на участь в ліквідації надзвичайних ситуацій та їх наслідків. Адміністрування вказаної системи та мобільного застосунку здійснюватимуть фахівці ДСНС України. В подальшому, у разі виникнення надзвичайної ситуації, система буде оповіщати зареєстрованих добровольців про місце та характеристики надзвичайної ситуації з урахуванням геолокації (місцезнаходження) добровольців. Крім того, в процесі ліквідації надзвичайної ситуації та її наслідків співробітники ДСНС України зможуть в режимі онлайн координувати дії добровольців, які першими прибудуть на місце події, надавати поради та застерігати їх від небезпечних дій до приїзду основних підрозділів ДСНС.

Таким чином, вищезазначена Система оповіщення та реагування «Я – доброволець» потребує належної адміністративно-правової регламентації та впровадження в практичну діяльність органів публічної адміністрації з використанням відповідного мобільного застосунку.

Поширення позитивного досвіду використання Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку на територію всієї держави дозволить всім бажаючим прийняти особисту участь в ліквідації надзвичайних ситуацій та їх наслідків, тобто проявити соціальну активність та отримати відповідний досвід роботи рятувальником. Водночас збільшення кількості потенційних добровольців та активне використання вказаного мобільного застосунку з урахуванням геолокації (місцезнаходження) користувачів дозволить оперативно мобілізувати людські та матеріально-технічні ресурси для ліквідації надзвичайних ситуацій.

Отже, на рівні спільного наказу МВС України та Міністерства цифрової трансформації України доцільно затвердити порядок функціонування

Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку.

Автором даного дослідження виконано науково-дослідну роботу в рамках якої розроблено та здійснено державну реєстрацію винаходу (корисної моделі) «Спосіб залучення добровольців до ліквідації наслідків надзвичайних подій засобами інноваційної інформаційної платформи».

В описі корисної моделі зазначено, шо Корисна модель відноситься до сфери забезпечення безпеки життєдіяльності людей в умовах надзвичайних ситуацій та надання допомоги у ліквідації їх наслідків шляхом організації та координування дій добровольців засобами інноваційної інформаційної платформи.

Зазначені відомі способи залучення добровольців до ліквідації наслідків надзвичайних подій в межах населених пунктів – за рішенням органів місцевого самоврядування, або на підприємствах, в установах та організаціях – за рішенням керівників, створюються підрозділи місцевої або добровільної пожежної охорони. Означені підрозділи, відповідно до покладених на них завдань, проводять заходи із запобігання виникненню пожеж, контролюють дотримання вимог пожежної безпеки, беруть участь в проведенні перевірок протипожежного стану об’єктів, здійснюють гасіння пожеж, проводять евакуацію людей та матеріальних цінностей, вживають заходів для мінімізації або ліквідації наслідків пожеж, зокрема разом з працівниками екстрених служб, вживають заходів для постійного підтримання своєї готовності до виконання покладених функцій тощо [225, 226]. Такий підхід до залучення населення до ліквідації надзвичайних ситуацій на добровільних засадах суттєво обмежує можливості добровольців через прив’язку до вказаного населеного пункту або об’єкта, не передбачає використання інформаційних технологій для управління діяльністю добровольців, унеможливлює залучення добровольців до широкого спектра подій (зокрема, ліквідації наслідків дорожньо-транспортних пригод, ідентифікації вибухонебезпечних предметів тощо), не дає змоги корегувати кількість залучених добровольців

залежно від масштабу події тощо. Зазвичай, оповіщення добровольців для залучення до ліквідації надзвичайних подій відбувається шляхом почергового дозвону засобами телефонії. Такий підхід збільшує загальний час оповіщення та створює перешкоди для своєчасного реагування.

Запропонована корисна модель «Спосіб залучення добровольців до ліквідації наслідків надзвичайних подій засобами інноваційної інформаційної платформи» за своїми характеристиками має низку переваг: забезпечення оповіщення добровольців для реагування на події засобами мобільних платформ (миттєві пуш-сповіщення у мобільний додаток); координація діяльності добровольців через мобільний застосунок; можливість самостійного обрання події для надання допомоги; можливість визначення дати, часу та зони відповідальності для реагування на надзвичайні події; можливість побудови маршруту слідування до місця події у разі підтвердження участі у наданні допомоги; наявність адміністративної складової для координування залучення добровольців, формування списків на оповіщення, обліку залученості, адміністрування бази даних надзвичайних подій; можливість обліку аналітичних даних про надзвичайні події, на ліквідацію яких залучались добровольці.

Суть винаходу – створення системи оповіщення та реагування на надзвичайні події на основі інформаційної системи, яка передбачає формування єдиної бази даних добровольців, їх залучення до ліквідації надзвичайних подій та координування дій шляхом використання мобільного додатка.

Робота системи оповіщення та реагування на надзвичайні події на основі інформаційної системи передбачає першочергове формування бази даних добровольців. Реєстрація у мобільному додатку можлива лише для осіб, які перебувають у базі даних. Це дасть змогу залучати до ліквідації надзвичайних ситуацій фахівців із відповідними освітою та рівнем підготовки. Мобільний додаток інформаційної системи дає змогу визначити дату, час та зону відповідальності, коли доброволець здатен долучатись до ліквідації

надзвичайних подій. Ці дані надсилаються та зберігаються в адміністративній частині системи. Для кожної події адміністратор системи визначає першочергову кількість добровольців для залучення. Система в автоматичному режимі надсилає сповіщення добровольцям на мобільні пристрої, відповідно до параметрів реєстрації (дата, час, місце). Зворотній зв'язок інтерфейсу мобільного застосунку дає змогу добровольцю зголоситись до участі в ліквідації надзвичайної події або відмовитись.

Відповідь надходить до адміністратора інформаційної системи і мобільний додаток автоматично будує найкоротший маршрут слідування до місця події.

За умови підтвердження необхідної кількості добровольців, система припиняє пошук і розсилку сповіщень. За умови відмови або не підтвердження участі необхідної кількості добровольців, система продовжує пошук в автоматичному режимі. Якщо число добровольців досягає кількості, встановленої адміністратором, додаток створює чергу та повідомляє усіх наступних добровольців про потрапляння до списку очікування. Потребу у залученні додаткової кількості добровольців під час ліквідування надзвичайної події, підтверджує спеціаліст – керівник ліквідації надзвичайної події за результатами оцінки обстановки. У разі підтвердження необхідності залучення більшої кількості добровольців, добровольці із списку очікування отримують про це повідомлення через мобільний додаток.

Запропонований спосіб дає можливість автоматизувати процеси залучення та координації дій добровольців під час ліквідації наслідків масштабних надзвичайних подій.

Окрім мобільних застосунків у сфері забезпечення безпеки життєдіяльності також активно використовується інше програмне забезпечення, яке дозволяє суттєво удосконалити процеси публічного управління у даній сфері суспільних відносин. Однією з перспективних інформаційних технологій, яка поступово впроваджується в діяльність органів публічної адміністрації, є технологія штучного інтелекту.

Так, в Концепції розвитку штучного інтелекту в Україні зазначено, що штучний інтелект – це організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [281].

Одним із перспективних напрямів використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності є кібербезпека. Так, як зазначено в Концепції розвитку штучного інтелекту в Україні, основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі штучного інтелекту є 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 [281].

До завдань, виконання яких дозволить вирішити актуальні проблеми кібербезпеки, віднесено зокрема удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик штучного інтелекту у сфері кібербезпеки і кіберзахисту [281].

Не менш важливим є використання технології штучного інтелекту для забезпечення інформаційної безпеки, яка є невід'ємною частиною механізму забезпечення безпеки життєдіяльності в цілому.

У відповідності до Концепції розвитку штучного інтелекту в Україні, застосування технологій штучного інтелекту в забезпеченні інформаційної безпеки є одним із факторів, що сприятиме забезпеченню національних інтересів. Зокрема, моніторинг соціальних мереж та інтернет-ресурсів електронних медіа з використанням технологій штучного інтелекту дає

можливість виявляти системні тренди і проблематику, діяти на випередження, аналізувати цільову аудиторію [281].

Технологія штучного інтелекту дозволяє в автоматичному режимі здійснювати виявлення та нейтралізацію реальних і потенційних загроз поширення засобами масової інформації та окремими користувачами Інтернет культу насильства та жорстокості, дитячої порнографії, а також намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення неповної, фейкової (недостовірної) або упередженої інформації.

Таким чином, використання технології штучного інтелекту для забезпечення інформаційної безпеки та кібербезпеки повинно мати чітку правову основу, адже протидія вищепереліченим негативним факторам є завданням органів публічної адміністрації, діяльність яких повинна здійснюватися виключно на підставі, на виконання та у відповідності до чинного законодавства. Наразі чинними є: Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII [269], Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 р. № 685/2021 [277] та Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 [276].

Крім того, технологія штучного інтелекту може використовуватись в автоматизованих системах запобігання та ліквідації надзвичайних ситуацій та їх наслідків. Це, зокрема, автоматизовані системи пожежогасіння, які на підставі забраної інформації, показань датчиків диму та результатів відеоспостереження, самостійно приймають рішення про цілеспрямоване застосування протипожежних засобів з метою локалізації та ліквідації займання.

Іншим прикладом використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності є використання автоматизованих систем моніторингу стану безпеки дорожнього руху, коли алгоритми штучного інтелекту аналізують всю зібрану інформацію з камер відеофіксації

порушень правил дорожнього руху, включаючи вимірювання швидкості транспортних засобів, та у випадку загрози настання аварійної ситуації (або за фактом її безпосереднього настання) самостійно приймають рішення про обмеження руху на певній ділянці дороги шляхом активації заборонених сигналів, знаків або блокування руху автоматизованими технічними засобами (болардами – гідравлічними висувними дорожніми блокувальниками).

Таким чином, існує об'єктивна потреба розробити та прийняти окремий Закон України «Про штучний інтелект», яким будуть врегульовані, у тому числі, основні питання використання даної інформаційної технології у сфері забезпечення безпеки життєдіяльності.

У випадку зволікання з прийняттям загального Закону України «Про штучний інтелект» доцільно розробити та прийняти Закон України «Про використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності» (як варіант – доповнити Розділ ІІ Кодексу цивільного захисту України новою главою «Використання технології штучного інтелекту в єдиній державні системі цивільного захисту»), яким буде врегульовано, зокрема, використання технології штучного інтелекту в єдиній державній системі цивільного захисту та в механізмі забезпечення безпеки життєдіяльності в цілому.

Ще однією інформаційною технологією, яка часто застосовується у сфері забезпечення безпеки життєдіяльності та потребує детальної адміністративно-правової регламентації, є технологія криптографічного захисту інформації. Особливої актуальності необхідність шифрування важливої інформації, включаючи персональні дані суб'єктів, перелік об'єктів та характеристики сил та засобів системи цивільного захисту, набула в умовах правового режиму воєнного стану, коли неприпустимим є розголошення даних про надзвичайні ситуації воєнного характеру, персональних даних рятувальників тощо.

В Енциклопедії сучасної України криптографічний захист інформації визначається як різновид захисту інформації з обмеженим

доступом, розголошення якої завдає (або може завдати) шкоди державі, суспільству чи особі. Криптографічний захист інформації реалізують шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. В Україні діє Положення про порядок здійснення криптографічного захисту інформації, затверджене Указом Президента України від 22 травня 1998 року 505/98 (із подальшими змінами та доповненнями) [80].

До засобів криптографічного захисту інформації належать апаратні, програмні та апаратно-програмні системи і комплекси, що реалізують криптографічні алгоритми перетворення інформації [80].

Правовою основою криптографічного захисту інформації є Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР [258]. Окремий проект Закону України «Про криптографічний та технічний захист інформації» був розроблений у 2016-му році, проте він так і не був прийнятий. Адміністративно-правове регулювання криптографічного захисту інформації в діяльності органів публічної адміністрації здійснюється на основі Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженого наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 (у редакції наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14.12.2015 № 767) [251].

Не менш важливим є забезпечення збереження важливої інформації у сфері забезпечення безпеки життєдіяльності на декількох альтернативних серверах. Причому таку інформацію варто зберігати не тільки на національних носіях, але й серверах, які розташовані в зарубіжних країнах, які мають надійні партнерські відносини з Україною.

Так, Законом України «Про основні засади забезпечення кібербезпеки України» перебачено, серед іншого, функціонування Національного центру

резервування державних інформаційних ресурсів як організованої сукупності об’єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій [269].

Перспективним напрямом використання програмного забезпечення у сфері забезпечення безпеки життєдіяльності є використання робототехніки, яка здатна замінити людину в процесі ліквідації особливо небезпечних надзвичайних ситуацій та їх наслідків. Так, роботи можуть використовуватися для виконання робіт на об’єктах та територіях, де само перебування людини є небезпечним внаслідок радіаційного, хімічного або біологічного зараження; для розмінування територій та об’єктів, які містять міни-пастки та боєприпаси, які не розірвалися та можуть здетанувати в будь-який момент; для проведення рятувальних робіт в зоні ведення бойових дій тощо. Належне програмне забезпечення з використанням елементів технології штучного інтелекту дозволяє розробити та використовувати наземні та літальні безпілотні апарати з «машинним зором», на які не діють засоби РЕБ (радіоелектронної боротьби) та які самостійно, без участі оператора, досягають запрограмованої цілі та виконують поставлене завдання.

Таким чином, перспективним напрямом удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності є правова регламентація використання робототехніки (та відповідного програмного забезпечення), яка здатна замінити людину в процесі ліквідації особливо небезпечних надзвичайних ситуацій та їх наслідків.

Отже, сучасні інформаційні технології дозволяють значно удосконалити національну систему цивільного захисту та механізми забезпечення безпеки життєдіяльності в цілому. До інноваційних інформаційних технологій, які

використовуються у сфері забезпечення безпеки життєдіяльності відносяться: мобільні застосунки, автоматизовані інформаційні системи, засоби робототехніки та відповідне програмне забезпечення, технологія штучного інтелекту.

Як вже було зазначено у попередніх підрозділах роботи, адміністративно-правове регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності доцільно здійснювати на рівні спільних наказів МВС України та Міністерства цифрової трансформації України, адже саме до компетенції останнього віднесено координацію діяльності інших органів публічної адміністрації у сфері цифровізації [222].

Так, з метою удосконалення національної системи цивільного захисту доцільно затвердити спільним наказом МВС України та Міністерства цифрової трансформації України порядок використання Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку, що сприятиме залученню соціально-активних громадян до ліквідації надзвичайних ситуацій та їх наслідків.

Отже, мобільні застосунки та інше програмне забезпечення, за умови належної адміністративно-правової регламентації, здатні суттєво удосконалити національну систему цивільного захисту та механізм забезпечення безпеки життєдіяльності в цілому.

Таким чином, перспективним напрямом удосконалення правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності є адміністративно-правова регламентація створення та порядку використання єдиної інформаційно-телекомунікаційної системи цивільного захисту та спеціального мобільного застосунку, основним завданням якого буде створення бази даних потенційних добровольців – осіб, які бажають прийняти участь в ліквідації надзвичайних ситуацій та їх наслідків, а також забезпечення функціонування ефективного механізму мобілізації зазначених добровольців з метою ліквідації конкретної

надзвичайної події (ситуації) та її наслідків з урахуванням геолокації, тобто залучення до ліквідації надзвичайної ситуації в першу чергу тих добровольців, які знаходяться (перебувають, проїжджають, проживають) поблизу місця події.

Правового врегулювання потребує і питання фінансового та матеріально-технічного забезпечення функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб'єктів, які на добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків.

Актуальним напрямом удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та цивільного захисту є цифровізація освітнього процесу, що включає використання інформаційних технологій в процесі навчання громадян основам безпеки життєдіяльності та цивільного захисту з метою підвищення рівня готовності громадян до виникнення потенційних надзвичайних ситуацій та засвоєння ними основних правил поведінки у названих ситуаціях.

Так, в Стратегії розвитку вищої освіти в Україні на 2022-2032 роки: розпорядження Кабінету Міністрів України від 23 лютого 2022 р. № 286-р. ідентифікована така проблема як низький рівень довіри до інноваційної діяльності закладів вищої освіти, недостатні практика та досвід впровадження цифрових технологій.

Також у вказаній Стратегії зазначається, що у 2020 році Європейська Комісія затвердила План дій з цифрової освіти на 2021-2027 роки, який передбачає такі два пріоритетних напрями, як прискорення розвитку ефективних цифрових освітніх екосистем, що потребує наявності розвинутої інфраструктури, зв'язку і цифрового обладнання, ефективного планування та

розвитку цифрового потенціалу, включаючи сучасні організаційні можливості, підготовлених наукових, науково-педагогічних та педагогічних працівників, які володіють цифровими компетентностями, високоякісного освітнього наповнення, інструментів і безпечних платформ, що відповідають стандартам приватності та етики та є зручними для користувачів, застосування допоміжних технологій для осіб з інвалідністю; розвиток цифрових умінь і компетентностей для цифрової трансформації, зокрема базових цифрових умінь і компетентностей, починаючи з дошкільного віку, поглиблених цифрових навичок, підготовка більшої кількості фахівців у цій сфері, зокрема з урахуванням гендерного балансу [284].

Таким чином, цифровізація освітнього процесу, включаючи навчання громадян основам безпеки життєдіяльності та цивільного захисту, повинна здійснюватися комплексно та включати як створення необхідної технічної інфраструктури, так і ознайомлення персоналу освітніх закладів з новітніми інноваційними інформаційними технологіями, які можуть бути використані як в освітньому процесу, так і безпосередньо у сфері забезпечення безпеки життєдіяльності та цивільного захисту.

Так, в Стратегії розвитку вищої освіти в Україні на 2022-2032 роки зазначається, що інноваційність повинна бути реалізована шляхом застосування нових та удосконалених методів і практик (включаючи цифрові технології) для викладання, навчання та оцінювання, що повинні здійснюватися у тісному зв’язку із дослідженнями. Заклади освіти повинні диверсифікувати освітні пропозиції та оновлювати зміст освіти з метою задоволення зростаючих потреб у розвитку інноваційного та критичного мислення, підприємницьких та лідерських навичок, розвивати гнучкі освітні траєкторії на основі студентоцентрованого підходу [284].

Взаємопов’язаність планується забезпечити шляхом сприяння міжнародній співпраці та реформам, обміну знаннями, академічній мобільності студентів і персоналу, набуттю учасниками освітнього процесу міжнаціональних та міжкультурних компетентностей. Не менш як 20 відсотків

випускників в Європейському просторі вищої освіти повинні пройти навчання за кордоном. Цифрові технології допоможуть здійснювати безпечний, ефективний та прозорий обмін даними (з урахуванням захисту приватності) і застосовуватимуться у сфері визнання кваліфікацій, забезпечення якості та мобільності з урахуванням досвіду реалізації, зокрема, ініціативи European Student Card [284].

Отже, ключову роль у провадженні інноваційних інформаційних технологій в освітній процес, включаючи викладання дисциплін «Безпека життєдіяльності» та «Цивільний захист», повинна відігравати міжнародна співпраця, академічна мобільність студентів і персоналу, набуття учасниками освітнього процесу міжнаціональних та міжкультурних компетентностей з акцентом на стандарти та технології, які використовуються в Європейському Союзі.

Крім того, в Стратегії розвитку вищої освіти в Україні на 2022- 2032 роки визначено завдання, спрямовані на досягнення поставлених цілей, механізми та етапи реалізації вказаної Стратегії. Так одним із завдань є цифрова трансформація процесів управління, регулювання та моніторингу в закладах вищої освіти та ефективне використання цифрових (дистанційних) технологій в освітньому процесі [284].

Отже, цифровізація освітнього процесу, включаючи викладання дисциплін, пов’язаних із безпекою життєдіяльності та цивільним захистом, повинна мати належне адміністративно-правове забезпечення у вигляді спільної нормотворчої діяльності Міністерства освіти і науки України, Міністерства цифрової трансформації України та центральних органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту.

Окремо слід наголосити на необхідності адміністративно-правового регулювання використання технології штучного інтелекту в освітньому процесі та у сфері забезпечення безпеки життєдіяльності. Належна правова регламентація повинна забезпечити однаковий (стандартизований) підхід до

використання інструментарію штучного інтелекту учасниками освітнього процесу та суб'єктами владних повноважень органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, керівниками та уповноваженими посадовими особами підприємств, установ та організацій незалежно від форми власності. Однаковий підхід забезпечить сумісність програмного забезпечення, а також унеможливить негативні наслідки від потенційного несанкціонованого втручання в роботу штучного інтелекту в чутливих сферах суспільних відносин, пов'язаних із забезпеченням безпеки життєдіяльності, тобто з високим ризиком завдання шкоди населенню чи природному середовищу у разі несанкціонованого втручання (остаточне рішення в таких випадках буде приймати людина).

Всі розглянуті вище актуальні питання адміністративно-правового регулювання використання інформаційних технологій доцільно врегулювати на рівні спільного наказу Міністерства внутрішніх справ України та Міністерства цифрової трансформації України, що забезпечить використання новітніх інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

Проведене дослідження актуальних напрямів удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволяє виділити наступні перспективні напрями нормотворчої діяльності:

- адміністративно правове врегулювання розробки та функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати, серед іншого, інтерактивну мапу захисних укриттів (з можливістю побудови маршруту слідування для особи з урахуванням геолокації), місць локалізації надзвичайних ситуацій та їх наслідків (за виключенням місць прильотів ворожих ракет та безпілотних літальних апаратів), а також інформаційну базу суб'єктів забезпечення цивільного захисту та безпеки життєдіяльності;

- адміністративно-правова регламентація розробки, поширення

(популяризації), а також порядку адміністрування і використання мобільного застосунку, призначеного для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації, а саме, затвердження спільним наказом МВС України та Міністерства цифрової трансформації України порядку використання Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку, що сприятиме залученню соціально-активних громадян до ліквідації надзвичайних ситуацій та їх наслідків;

- адміністративно-правове визначення системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які будуть здійснювати адміністрування єдиної інформаційно-телекомунікаційної системи цивільного захисту, а також здійснювати оперативне обслуговування (керування центром управління) мобільних застосунків, призначених для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації;

- адміністративно-правове врегулювання питання фінансового та матеріально-технічного забезпечення функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб'єктів, які на добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків;

- прийняття окремого Закону України «Про штучний інтелект», яким будуть врегульовані, у тому числі, основні питання використання технології штучного інтелекту в єдиній державній системі цивільного захисту та в механізмі забезпечення безпеки життєдіяльності в цілому, а також адміністративно-правове врегулювання порядку використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності на рівні підзаконних (відомчих) нормативно-правових актів;

- адміністративно-правову регламентацію збереження важливої інформації у сфері цивільного захисту та забезпечення безпеки життєдіяльності на декількох альтернативних серверах, включаючи сервери, які розташовані в зарубіжних країнах, що мають надійні партнерські відносини з Україною;

- адміністративно-правове регулювання цифровізації освітнього процесу, що включає використання інформаційних технологій в процесі навчання громадян основам безпеки життєдіяльності та цивільного захисту з метою підвищення рівня готовності громадян до виникнення потенційних надзвичайних ситуацій та засвоєння ними основних правил поведінки у названих ситуаціях;

- адміністративно-правову регламентацію використання робототехніки, яка здатна замінити людину в процесі ліквідації особливо небезпечних надзвичайних ситуацій та їх наслідків.

Висновки до розділу 4

1. Проведене дослідження адміністративно-правових засад цифровізації системи публічного управління в Україні дозволяє сформулювати висновок про те, що існує об’єктивна необхідність адміністративно-правового регулювання тих інформаційних технологій, які безпосередньо зачіпають права і свободи людини та можуть негативно впливати на безпеку життєдіяльності людини та суспільства в цілому.

Зокрема, об’єктивною є потреба детальної регламентації використання технології штучного інтелекту з метою недопущення його неконтрольованого використання юридичними та фізичними особами у найбільш чутливих сферах суспільних відносин, зокрема, в медицині, військовій сфері, у сфері охорони правопорядку.

2. Проведене дослідження правових засобів забезпечення безпеки життєдіяльності в контексті цифровізації публічного управління дозволяє

зробити висновок про те, що правові засоби забезпечення безпеки життєдіяльності у більшій частині є адміністративними, постійно діючими на території всієї держави, загальними, публічно-правовими, імперативними, такими, що більшою мірою зобов'язують та забороняють, обмежуючими.

Також слід відзначити, що адміністративно-правове врегулювання використання сучасних інформаційних технологій у сфері забезпечення безпеки життєдіяльності за допомогою адміністративно-правових засобів дозволить уніфікувати порядок використання інноваційних цифрових інструментів, що в свою чергу забезпечить сумісність програмного забезпечення в процесі взаємодії різних суб'єктів в системі цивільного захисту, а також сприятиме поширенню позитивного досвіду практичного застосування вказаних цифрових інструментів окремими суб'єктами владних повноважень на територію всієї держави.

Крім того, за результатами проведеного дослідження слід наголосити на необхідності внесення змін до чинного національного адміністративного законодавства в частині правової регламентації використання інструментарію технології штучного інтелекту, а також використання можливостей мобільних застосунків у сфері забезпечення безпеки життєдіяльності. Зокрема, пропонується розробити та прийняти відповідний національний закон про штучний інтелект, яким будуть врегульовані всі можливі аспекти використання даної інформаційної технології у різних сферах суспільних відносин, включаючи сферу забезпечення безпеки життєдіяльності.

Також пропонується спільним наказом Міністерства внутрішніх справ України та Міністерства цифрової трансформації України затвердити порядок використання перспективного мобільного застосунку «Надзвичайна ситуація», призначеного для мобілізації людських та матеріально-технічних ресурсів з метою ліквідації надзвичайних ситуацій та їх наслідків.

3. Проведене дослідження актуальних напрямів удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволяє виділити

наступні перспективні напрями нормотворчої діяльності:

- адміністративно правове врегулювання розробки та функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати, серед іншого, інтерактивну мапу захисних укриттів (з можливістю побудови маршруту слідування для особи з урахуванням геолокації), місць локалізації надзвичайних ситуацій та їх наслідків, а також інформаційну базу суб'єктів забезпечення цивільного захисту та безпеки життєдіяльності;

- адміністративно-правова регламентація розробки, поширення (популяризації), а також порядку адміністрування і використання мобільного застосунку, призначеного для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації, а саме, затвердження спільним наказом МВС України та Міністерства цифрової трансформації України порядку використання Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку, що сприятиме залученню соціально-активних громадян до ліквідації надзвичайних ситуацій та їх наслідків;

- адміністративно-правове визначення системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які будуть здійснювати адміністрування єдиної інформаційно-телекомунікаційної системи цивільного захисту, а також здійснювати оперативне обслуговування (керування центром управління) мобільних застосунків, призначених для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації;

- адміністративно-правове врегулювання питання фінансового та матеріально-технічного забезпечення функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб'єктів, які на

добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків;

- прийняття окремого Закону України «Про штучний інтелект», яким будуть врегульовані, у тому числі, основні питання використання технології штучного інтелекту в єдиній державній системі цивільного захисту та в механізмі забезпечення безпеки життєдіяльності в цілому, а також адміністративно-правове врегулювання порядку використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності на рівні підзаконних (відомчих) нормативно-правових актів;

- адміністративно-правову регламентацію збереження важливої інформації у сфері цивільного захисту та забезпечення безпеки життєдіяльності на декількох альтернативних серверах, включаючи сервери, які розташовані в зарубіжних країнах, що мають надійні партнерські відносини з Україною;

- адміністративно-правове регулювання цифровізації освітнього процесу, що включає використання інформаційних технологій в процесі навчання громадян основам безпеки життєдіяльності та цивільного захисту з метою підвищення рівня готовності громадян до виникнення потенційних надзвичайних ситуацій та засвоєння ними основних правил поведінки у названих ситуаціях;

- адміністративно-правову регламентацію використання робототехніки, яка здатна замінити людину в процесі ліквідації особливо небезпечних надзвичайних ситуацій та їх наслідків.

Наведений перелік перспективних напрямів нормотворчої діяльності щодо правової регламентації використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності не є вичерпним, адже у світі продовжується активних розвиток цифрових технологій, тільки починається ера використання можливостей штучного інтелекту.

ВИСНОВКИ

У дисертаційному дослідженні на основі комплексного аналізу теоретичних напрацювань у сфері безпеки життєдіяльності, адміністративного та інформаційного права, положень чинного національного законодавства, а також адміністративної практики його реалізації здійснено теоретичне узагальнення, а також сформульовано науково обґрунтовані висновки і практичні рекомендації, які розв'язують наукову проблему щодо вдосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. За результатами дослідження сформульовано такі висновки:

1. За результатами аналізу історіографії проблематики адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності виділено чотири групи наукових літературних джерел. До першої групи віднесено підручники, навчальні посібники, монографії, публікації у періодичних виданнях, присвячені питанням забезпечення безпеки життєдіяльності, підготовлені фахівцями з прикладних, технічних та природничих наук. До другої групи віднесено наукові видання, монографії, дисертаційні дослідження, присвячені питанням використання інформаційних технологій у різних сферах суспільних відносин, включаючи основні напрями та способи цифровізації, використання цифрових інструментів для досягнення публічних та приватних цілей учасників суспільних відносин, надання цифрових послуг тощо. До третьої групи віднесено дослідження, присвячені адміністративно-правовому регулюванню інформаційних відносин, включаючи адміністративно-правові засади інформатизації, використання цифрових інструментів, надання цифрових адміністративних послуг, а також правове регулювання порядку збирання, зберігання та використання інформації в комп'ютерних мережах, питання відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем,

електронних комунікаційних мереж, правове регулювання Інтернету, технології штучного інтелекту та інших інформаційних технологій. До четвертої групи віднесено дослідження науковців, присвячені організації публічного управління та правовому регулюванню у сфері забезпечення безпеки життєдіяльності.

2. Зазначено, що аналіз методології дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволив сформулювати висновок про необхідність органічного поєднання в процесі наукового пошуку законів, прийомів та принципів діалектики, основних загальнонаукових та спеціально-юридичних методів дослідження, а також доцільність використання провідних наукових підходів: цивілізаційного, антропологічного (антропоцентричного), інструментального, телеологічного та синергетичного, що дасть можливість врахувати всі об’єктивні і суб’єктивні чинники, які впливають на особливості використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності та зумовлюють необхідність адміністративно-правової регламентації їх використання.

Встановлено, що з точки зору синергетики механізм забезпечення безпеки життєдіяльності є складною системою, що здатна до самоорганізації та самовдосконалення, тому завданням органів публічної адміністрації є встановлення закономірностей, які впливають на формування та розвиток вказаної системи та закріплення їх у правовій формі з метою забезпечення їх охорони та підтримки з боку держави. Зокрема, цифровізація суспільних відносин у сфері забезпечення безпеки життєдіяльності є об’єктивною тенденцією, проте саме адміністративно-правове регулювання впровадження інформаційних технологій у вказану сферу суспільних відносин гарантує стабільний розвиток усієї системи та уніфіковані правила взаємодії між усіма суб’єктами, забезпечує централізований захист інформаційних ресурсів та оперативне поширення позитивного досвіду використання цифрових інструментів.

3. Визначено, що проведене дослідження історії становлення та розвитку адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності дозволило сформулювати висновок, що в Україні відбулася низка реформ органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, включаючи демілітаризацію військ цивільної оборони, що в результаті призвело до утворення нині діючої Державної служби України з надзвичайних ситуацій, діяльність якої спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ.

В історії цифровізації діяльності органів публічної адміністрації, включаючи впровадження інформаційних технологій у діяльність Державної служби України з надзвичайних ситуацій, можна умовно виділити чотири основних етапи, останній з яких характеризується активним впровадженням інноваційних інформаційних технологій у сферу забезпечення безпеки життєдіяльності та цивільного захисту, що включає: використання технології штучного інтелекту та можливостей мобільних застосунків, створення автоматизованих інтегрованих інформаційних систем цивільного захисту тощо.

З урахуванням дослідженого історичного досвіду пропонується розробити та впровадити в практичну діяльність ДСНС окрему інформаційну систему цивільного захисту з інтегрованою інтерактивною картою надзвичайних ситуацій та подій, які відбувались та відбуваються на території України, інтерактивною картою укриттів (захисних споруд) для населення на час повітряної тривоги з можливістю побудови маршруту до них з урахуванням геолокації користувача, а також інформаційною базою добровольців з використанням спеціального мобільного застосунку «Я – доброволець», що дозволить оперативно мобілізувати бажаючих взяти участь у ліквідації актуальної надзвичайної ситуації та її наслідків.

4. Охарактеризовано, що систематизація адміністративно-правових засад побудови системи цивільного захисту та забезпечення безпеки

життєдіяльності в Україні дозволила сформулювати висновок, що правовою основою адміністративно-правового регулювання у сферах забезпечення безпеки життєдіяльності та цивільного захисту є Конституція України, рішення Конституційного Суду України та ратифіковані Верховною Радою України міжнародні нормативно-правові акти, кодекси та закони України, правові висновки (позиції) Верховного Суду. Натомість зміст адміністративно-правового регулювання у вказаній сфері суспільних відносин становлять укази Президента України та постанови Кабінету Міністрів України, накази МВС України та Державної служби України з надзвичайних ситуацій, спільні накази органів публічної адміністрації, а також акти органів місцевого самоврядування.

Особливістю адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту є досить часті випадки спільної нормотворчої діяльності органів публічної адміністрації з метою забезпечення обміну інформацією про надзвичайні ситуації та координації діяльності з ліквідації надзвичайних ситуацій та їх наслідків. Також особливістю адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту є часте використання техніко-юридичних (технічних) норм у підзаконних актах.

Окремо слід підкреслити необхідність адміністративно-правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності з метою забезпечення сумісності програмного забезпечення, централізованого захисту інформації та поширення позитивного досвіду використання інноваційних інформаційних технологій у вказаній сфері суспільних відносин.

5. Встановлено, що заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій досить детально регламентовані Кодексом цивільного захисту України та Законом України «Про правовий режим надзвичайного стану». Крім того, вказані заходи передбачені підзаконними нормативно-правовими актами, серед яких: Концепція захисту

населення і територій у разі загрози та виникнення надзвичайних ситуацій, схвалена указом Президента України від 26 березня 1999 р. № 284/99, Положення про Державну службу України з надзвичайних ситуацій, затверджене постановою Кабінету Міністрів України від 16 грудня 2015 р. № 1052, Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, затверджене постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733.

6. Встановлено, що дослідження системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволило зробити висновок, що з урахуванням зростаючих загроз природного, техногенного, соціального та воєнного характеру є реальна потреба створення єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати інтерактивну мапу та інформаційну базу суб'єктів забезпечення цивільного захисту. Також є об'єктивна потреба нормативного визначення системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які будуть здійснювати адміністрування вказаної інформаційно-телекомунікаційної системи, відповідної бази даних, а також здійснювати оперативне обслуговування (керування центром управління, штабом) мобільних застосунків, призначених для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення чи безпосереднього виникнення надзвичайної ситуації.

Таким чином, є необхідність внесення змін до чинного національного законодавства щодо адміністративно-правової регламентації створення єдиної інформаційно-телекомунікаційної системи цивільного захисту, а також адміністративно-правової регламентації використання мобільних застосунків у сфері забезпечення безпеки життєдіяльності, включаючи права та обов'язки суб'єктів, які будуть здійснювати адміністрування вказаних мобільних застосунків, а також суб'єктів, які будуть залучатися до ліквідації

надзвичайних ситуацій та їх наслідків як добровольців з використанням встановленого мобільного застосунку.

Правового врегулювання потребує і питання фінансового та матеріально-технічного забезпечення функціонування вищезазначеної єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб'єктів, які на добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків.

Зазначені питання доцільно врегулювати на рівні спільного наказу Міністерства внутрішніх справ України та Міністерства цифрової трансформації України, що забезпечить використання новітніх інформаційних технологій у сфері забезпечення безпеки життєдіяльності.

7. Визначено, що проведене дослідження позитивного досвіду адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі дає підстави сформулювати висновок, що в Механізмі цивільного захисту Європейського Союзу використовуються такі інформаційні технології, як інформаційні платформи, бази даних, засоби оперативного зв'язку та координації тощо. Використання вказаних інформаційних технологій має належну правову регламентацію на рівні рішень Європейського парламенту та Європейської Ради.

До правових засад використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності слід віднести GDPR – Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних, а також Європейський закон (Регламент) про штучний інтелект (Artificial Intelligence Act, AI Act).

Важливими документами щодо регулювання розвитку цифровізації в Європейському Союзі також є Європейська структура сумісності (EIF), яка надає загальний набір стандартів для забезпечення легкого доступу до державних послуг і спільного використання в усьому ЄС, а також Регламент eIDAS, що визначає правила електронної ідентифікації та довірчих послуг у всьому ЄС.

З огляду на необхідність завершення процесів євроінтеграції, національним органам публічної адміністрації, зокрема Міністерству цифрової трансформації України, необхідно активізувати участь національних державних та приватних інституцій у розвитку Єдиного цифрового ринку ЄС, залучати інвестиції для розвитку національного цифрового ринку, включаючи фінансування заходів із забезпечення кібербезпеки. Крім того, одним із завдань є завершення процедур адаптації національного законодавства в частині правового регулювання використання інформаційних технологій та забезпечення безпеки життєдіяльності до права ЄС.

8. Охарактеризовано, що проведене дослідження особливостей адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту у Сполучених Штатах Америки дає підстави сформулювати висновок про можливість та доцільність запозичення позитивного досвіду органів публічної адміністрації Сполучених Штатів Америки в частині адміністративно-правової регламентації діяльності у сфері цивільного захисту населення і територій від надзвичайних ситуацій. Зокрема, до позитивного досвіду слід віднести розробку та реалізацію FEMA Федерального плану, який є головним актом у процесі реагування на надзвичайну ситуацію та ліквідацію її наслідків. Також позитивним є досвід побудови структури та організації діяльності Федерального агентства з управління надзвичайними ситуаціями (FEMA), зокрема його функції щодо адміністрування та координації діяльності інших органів публічної адміністрації у вказаній сфері суспільних відносин.

Варто запозичити, зокрема, структуру та зміст офіційного сайту FEMA, який містить детальну інформацію як для суб'єктів владних повноважень, так і для громадян щодо організації цивільного захисту населення та територій Сполучених Штатів Америки від надзвичайних ситуацій.

На увагу заслуговує також досвід FEMA у сфері координації діяльності органів публічної адміністрації щодо своєчасного реагування на надзвичайні ситуації та оперативної ліквідації їх негативних наслідків, а також акумулювання інформації про надзвичайні ситуації, що забезпечується засобами комунікації з використанням новітніх інноваційних інформаційних технологій (швидкісного оптоволоконного зв'язку, захищеного серверного обладнання, хмарних технологій, можливостей соціальних мереж та месенджерів, технології штучного інтелекту тощо).

Позитивний досвід Сполучених Штатів Америки щодо розробки та реалізації Федерального плану реагування на надзвичайні ситуації доцільно врахувати в процесі нормотворчої діяльності щодо вдосконалення національного Плану реагування на надзвичайні ситуації державного рівня, затвердженого постановою Кабінету Міністрів України від 14 березня 2018 р. № 223.

9. Встановлено, що проведене дослідження адміністративно-правових засад забезпечення безпеки життєдіяльності та цивільного захисту в Японській Державі в умовах цифровізації дозволяє сформулювати висновок про доцільність запозичення трирівневої системи публічного управління ліквідацією надзвичайних ситуацій та їх наслідків у Японській Державі, в якій ключову роль відіграє рівень муніципалітетів, тобто організація сил та засобів цивільного захисту на рівні органів місцевого самоврядування, що дозволяє максимально оперативно реагувати на початок надзвичайної ситуації, а також проводити систематичні навчання та тренінги із населенням у сфері цивільного захисту.

Також слід підкреслити сталість національного законодавства Японської Держави та стабільність функціонування органів публічної

адміністрації, які реалізують державну політику Японської Держави у сфері забезпечення пожежної безпеки. Цей досвід вартий запозичення Україною, адже постійні реформи центральних органів виконавчої влади, включаючи органи публічної адміністрації, які реалізують державну політику у сфері цивільного захисту, не сприяють їх ефективній роботі, що включає формування традицій, злагодженості та згуртованості колективів, внутрішньої субкультури тощо.

Позитивним є досвід Японської Держави щодо створення «муніципальних корпорацій» або «асоціацій районів» з метою консолідації фінансових та організаційних ресурсів для ліквідації надзвичайних ситуацій. Також позитивним є досвід щодо функціонування волонтерських пожежних корпусів, які складаються із пожежних-волонтерів, які мають власну трудову діяльність або зайняті на іншій найманій роботі (однак у разі пожежі або іншої надзвичайної ситуації посадові особи та інші члени волонтерських пожежних корпусів повинні дотримуватися розпоряджень начальника пожежного департаменту або пожежної станції).

На увагу заслуговує також ізраїльська національна безпекова доктрина, ефективність існування якої підтверджена під час захисту цивільного населення в умовах воєнного протистояння, що постійно триває. Для України, яка перебуває у схожій ситуації, актуальною є ізраїльська модель поєднання сил та засобів органів військового управління та цивільних органів публічної адміністрації в організації ліквідації надзвичайних ситуацій та їх наслідків, включаючи використання сучасних інформаційних технологій у сфері забезпечення безпеки життєдіяльності, а саме новітніх систем оповіщення цивільного населення про загрозу ракетних обстрілів. Воєнно-орієнтований підхід до управління в умовах кризових ситуацій в Державі Ізраїль заслуговує на більш детальне дослідження та імплементацію в національне законодавство та юридичну практику. Позитивним також є досвід Держави Ізраїль щодо залучення добровольців-пожежників для ліквідації надзвичайних ситуацій.

10. Визначено, що проведене дослідження адміністративно-правових засад цифровізації системи публічного управління в Україні дозволяє сформулювати висновок про те, що наявна об'єктивна необхідність адміністративно-правового регулювання тих інформаційних технологій, які безпосередньо зачіпають права і свободи людини та можуть негативно впливати на безпеку життєдіяльності людини та суспільства загалом. Зокрема, об'єктивною є потреба детальної регламентації використання технології штучного інтелекту з метою недопущення його неконтрольованого використання юридичними та фізичними особами у найбільш чутливих сферах суспільних відносин, зокрема, в медицині, військовій сфері, у сфері охорони правопорядку.

Адміністративно-правового регулювання потребують також інформаційні технології, які використовуються в механізмі забезпечення безпеки життєдіяльності, зокрема в діяльності органів публічної адміністрації, які реалізують державну політику у сфері цивільного захисту. Необхідність адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності зумовлена у тому числі вимогою ст. 19 Конституції України, згідно з якою органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

11. Охарактеризовано, що проведене дослідження правових засобів забезпечення безпеки життєдіяльності в контексті цифровізації публічного управління дозволяє зробити висновок, що правові засоби забезпечення безпеки життєдіяльності у більшій частині є адміністративними, постійно діючими на території всієї держави, загальними, публічно-правовими, імперативними, такими, що більшою мірою зобов'язують та забороняють, обмежуючими.

Також слід відзначити, що адміністративно-правове врегулювання використання сучасних інформаційних технологій у сфері забезпечення

безпеки життєдіяльності за допомогою адміністративно-правових засобів дозволить уніфікувати порядок використання інноваційних цифрових інструментів, що своєю чергою забезпечить сумісність програмного забезпечення в процесі взаємодії різних суб'єктів у системі цивільного захисту, а також сприятиме поширенню позитивного досвіду практичного застосування вказаних цифрових інструментів окремими суб'єктами владних повноважень на територію всієї держави.

Крім того, за результатами проведеного дослідження підкреслено необхідність внесення змін до чинного національного адміністративного законодавства в частині правової регламентації використання інструментарію технології штучного інтелекту, а також використання можливостей мобільних застосунків у сфері забезпечення безпеки життєдіяльності. Зокрема, запропоновано розробити та прийняти відповідний національний закон про штучний інтелект, яким будуть врегульовані всі можливі аспекти використання такої інформаційної технології у різних сферах суспільних відносин, включаючи сферу забезпечення безпеки життєдіяльності.

12. Встановлено, що проведене дослідження актуальних напрямів удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності дозволяє виділити такі перспективні напрями нормотворчої діяльності:

– адміністративно-правове врегулювання розробки та функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, яка буде включати, серед іншого, інтерактивну мапу захисних укриттів (з можливістю побудови маршруту слідування для особи з урахуванням геолокації), місць локалізації надзвичайних ситуацій та їх наслідків (за виключенням місць прильотів ворожих ракет та безпілотних літальних апаратів), а також інформаційну базу суб'єктів забезпечення цивільного захисту та безпеки життєдіяльності;

– адміністративно-правова регламентація розробки, поширення (популяризації), а також порядку адміністрування і використання мобільного

застосунку, призначеного для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації, а саме затвердження спільним наказом МВС України та Міністерства цифрової трансформації України порядку використання Системи оповіщення та реагування «Я – доброволець» та відповідного мобільного застосунку, що сприятиме залученню соціально-активних громадян до ліквідації надзвичайних ситуацій та їх наслідків;

– адміністративно-правове визначення системи суб'єктів використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, які будуть здійснювати адміністрування єдиної інформаційно-телекомунікаційної системи цивільного захисту, а також здійснювати оперативне обслуговування (керування центром управління) мобільних застосунків, призначених для мобілізації людських та матеріально-технічних ресурсів у випадку загрози виникнення чи безпосереднього виникнення надзвичайної ситуації;

– адміністративно-правове врегулювання питання фінансового та матеріально-технічного забезпечення функціонування єдиної інформаційно-телекомунікаційної системи цивільного захисту, мобільного застосунку для мобілізації людських та матеріально-технічних ресурсів у разі загрози виникнення або безпосереднього виникнення надзвичайної ситуації, а також питання фінансового та матеріально-технічного забезпечення суб'єктів, які на добровільних засадах будуть залучатись до ліквідації надзвичайних ситуацій та їх наслідків;

– прийняття окремого Закону України «Про штучний інтелект», яким будуть врегульовані у тому числі основні питання використання технології штучного інтелекту в єдиній державній системі цивільного захисту та в механізмі забезпечення безпеки життєдіяльності загалом, а також адміністративно-правове врегулювання порядку використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності на рівні підзаконних (відомчих) нормативно-правових актів;

– адміністративно-правову регламентацію збереження важливої інформації у сфері цивільного захисту та забезпечення безпеки життєдіяльності на декількох альтернативних серверах, включаючи сервери, які розташовані в зарубіжних країнах, що мають надійні партнерські відносини з Україною;

– адміністративно-правову регламентацію використання робототехніки, яка здатна замінити людину в процесі ліквідації особливо небезпечних надзвичайних ситуацій та їх наслідків;

– адміністративно-правове регулювання цифровізації освітнього процесу, що включає використання інформаційних технологій у процесі навчання громадян основ безпеки життєдіяльності та цивільного захисту з метою підвищення рівня готовності громадян до виникнення потенційних надзвичайних ситуацій та засвоєння ними основних правил поведінки у названих ситуаціях;

– встановлення адміністративної відповідальності за невиконання встановленого порядку поведінки під час оголошення повітряної тривоги в публічних місцях, на підприємствах, установах та організаціях, незалежно від форми власності, що потребує внесення змін до чинного Кодексу України про адміністративні правопорушення та затвердження перспективного Порядку поведінки в публічних місцях, на підприємствах, установах та організаціях, незалежно від форми власності, під час повітряної тривоги.

Наведений перелік перспективних напрямів нормотворчої діяльності щодо правового врегулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності не є вичерпним, адже майже щодня з’являються нові інноваційні інформаційні технології, які потенційно можуть бути використані в механізмі забезпечення безпеки життєдіяльності людини та в єдиній державній системі цивільного захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративістика в умовах цифровізації: теорія, правове регулювання, практика: монографія / авт. колектив: С.В. Ківалов, Л.Р. Біла-Тіунова, Т.А. Латковська та ін. Одеса: Видавничий дім «Гельветика», 2022. 800 с.

2. Адміністративне право України. Академічний курс: підручник; за ред. Т.О. Коломоєць. К.: Юрінком Інтер, 2011. 576 с.

3. Адміністративне право України: академ. курс у 2-х томах / Авер'янов В.Б., Андрійко О.Ф., Битяк Ю.П., Голосніченко І.П., Ківалов С.В.; відп. ред. В.Б. Авер'янов; НАН України; Інститут держави і права ім. В.М. Корецького. К. : Юридична думка, 2007. Т. 1: Загальна частина. К.: Юридична думка, 2007. 591 с.

4. Адміністративне право України. Загальна частина: навч. посібник / О.І. Остапенко, М.В. Ковалів, С.С. Єсімов, Л.С. Гулак, Н.Я. Отчак, Л.О. Остапенко. Львів: СПОЛОМ, 2019. 504 с.

5. Адміністративне право України: навчальний посібник у 2-х томах / Галунько В.В., Олефір В.І., Пихтін М.П. та ін.; за заг. ред. В.В. Галунька. Херсон: ПАТ «Херсонська міська друкарня», 2011. Т.1: Загальне адміністративне право. 320 с.

6. Адміністративне право України: підручник / Ю.П. Битяк, В.М. Гаращук, О.В. Дьяченко та ін.; за заг. ред. Ю.П. Битяка. К.: Юрінком Інтер, 2007. 544 с.

7. Андрєєва О.М. Електронне урядування: теорія та практика: навчальний посібник. К.: Авега, 2015. 228 с.

8. Андрощук О.В., Кондратенко Ю.В., Головченко О.В., Ворона Т.О., Петрушен М.В. Інформаційні технології та їх вплив на розвиток суспільства. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2014. № 1. С. 42-47.

9. Антикорупційна стратегія на 2021-2025 роки. Національне агентство з питань запобігання корупції: офіційний веб-сайт. URL: https://nazk.gov.ua/wp-content/uploads/2022/08/Antykoruptsijna-strategiya-na-2021-2025-rr.pdf

10. Антонюк В.В. Елементи діджиталізації адміністративного судочинства України. *Діджиталізація та права людини* : збірник тез Міжнародної науково-практичної інтернет-конференції (м. Хмельницький, 30 берез. 2021 р.). Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова, 2021. С. 9-12.

11. Апшай Ф.В., Халак О.В. Аналіз правових засад безпеки життєдіяльності. *Journal «ScienceRise: Juridical Science»*. 2021. № 1 (15). С. 4-7. DOI: 10.15587/2523-4153.2021.228246

12. Арламов О.Ю. Безпека життєдіяльності та цивільний захист: конспект лекцій. Інститут енергозбереження та енергоменеджменту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». К., 2018. 93 с. URL: https://opcb.kpi.ua/wp-content/uploads/2014/09/BZDCZkonspekt.pdf (дата звернення: 07.11.2024).

13. Артем'єв С.Р., Малько О.Д. Цивільний захист як чинник системи забезпечення національної безпеки. *Наука і правоохорона*. 2018. № 2. С. 42-49.

14. Базові аспекти цифровізації та їх правове забезпечення: монографія / К.В. Єфремова, Д.І. Шматков, В.П. Кохан та ін.; за ред. К. В. Єфремової. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. 180 с.

15. Баєв О.О. Сфера інформаційних відносин України як об'єкт правового регулювання. *Правова інформатика.* 2011. № 1(29). С. 37-42.

16. Бака О.Ю. Історія виникнення і розвитку поняття «публічний інтерес» у законодавстві і юридичній практиці. *Науковий вісник Національного університету біоресурсів і природокористування України*. Серія: Право. 2015. Вип. 213 (1). С. 148-155.

17. Баран М.В. Інформаційна безпека як предмет адміністративно-правового регулювання. *Соціально-правові студії*. 2021. Випуск 3 (13). С. 50-56.

18. Балинська О.М., Ященко В.А. Синергетика як методологічна парадигма юридичних досліджень. *Науковий вісник Львівського державного університету внутрішніх справ*. 2017. № 4. С. 3-12.

19. Барило О.Г. Цивільний захист України як функція держави. *Інвестиції: практика та досвід.* 2017. № 16. С. 115-119.

20. Барікова А.А. Електронна держава: нова ефективність урядування: монографія. Київ : Юрінком Інтер, 2016. 224 с.

21. Бебик В.М. Глобальне інформаційне суспільство: поняття, структура, комунікації. *Інформація і право*. 2011. № 1 (1). С. 41-49. URL: https://ippi.org.ua/bebik-vm-globalne-informatsiine-suspilstvo-ponyattya-struktura-komunikatsii (дата звернення: 08.11.2024).

22. Беззубов Д.О. Суспільна безпека (організаційно-правові засади забезпечення): монографія. Київ: «МП Леся», 2013. 452 с.

23. Безпека життєдіяльності та охорона праці: навчальний посібник для здобувачів вищої освіти із галузі знань 08 «Право», спеціальність 081 «Право». Львів: Львівський державний університет внутрішніх справ, 2022. 219 с.

24. Белова І., Ярощук О., Гомотюк А. Розвиток процесів цифровізації в Європейському Союзі: перспективний досвід для України. *Економічний аналіз*. 2023. Том 33. № 1. С. 180-191. DOI: https://doi.org/10.35774/econa2023.01.180

25. Бенедек В., Кеттеман М. Свобода вираження поглядів та Інтернет. Париж: Вид-во Ради Європи, 2013. 204 с.

26. Берназюк О. Роль та місце цифрових технологій у сфері публічного управління. *Інформаційне право*. 2017. №10. URL: http://pgp-journal.kiev.ua/archive/2017/10/35.pdf (дата звернення: 07.08.2024).

27. Берназюк О.О. Цифрові технології у праві: сучасний погляд у майбутнє: монографія. Ужгород: Гельветика, 2020. 525 с.

28. Берназюк О.О. Цифрові технології у праві: тенденції та перспективи розвитку: автореф. дис. … д-ра юрид. наук: 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право». Ужгород, 2021. 34 с.

29. Бесчастний В.М. Державне управління в сфері безпеки дорожнього руху: монографія. Донецьк: ДЮІ ЛДУВС ім. Е.О. Дідоренка, 2011. 473 с.

30. Бєлоусов А.В. Методологічні аспекти удосконалення системи державного управління ризиками надзвичайних ситуацій. *Інвестиції : практика та досвід.* 2014. № 11. С. 131-134.

31. Біленська Д.О. Адміністративно-правове регулювання інформаційних відносин в Україні: автореф. дис. ... канд. юрид. наук: 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право»; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2016. 20 с.

32. Біліченко С.П. Інформаційні технології як інструментарій сучасних трансформаційних зрушень у розвитку регіонів. *Економічні інновації*. 2011. Вип. 43. С. 33-37.

33. Благодарний А. Методологія дослідження правової регламентації адміністративно-юрисдикційної діяльності правоохоронних органів. *Підприємництво, господарство і право.* 2018. № 6. С. 147-151.

34. Богданов Є.П. Особливості проведення інформаційно-просвітницької роботи з питань цивільного захисту та безпеки життєдіяльності. *Інноваційна педагогіка.* 2022. Вип. 47. С. 32-36.

35. Бойко В.В. Правове регулювання штучного інтелекту: міжнародний досвід. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування*. 2024. Том 35 (74) № 2. С. 23-29.

36. Боліла С. Роль інформаційних технологій та цифрових інструментів в умовах викликів війни та післявоєнного відновлення економіки України. *Таврійський науковий вісник. Серія: Економіка*. 2023. № 16. С. 265-275. https://doi.org/10.32782/2708-0366/2023.16.35

37. Бондар Д.В. Використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності: адміністративно-правові засади. *Право та державне управління.* 2024. № 3. С. 13-20. DOI: https://doi.org/10.32782/pdu.2024.3.2

38. Бондар Д.В. Заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій: адміністративно-правова регламентація та напрями удосконалення в умовах цифровізації. *Актуальні проблеми вітчизняної юриспруденції.* 2024. № 4. С. 46-54. DOI: https://doi.org/10.32782/2408-9257-2024-4-8

39. Бондар Д.В. Історіографія та методологія дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал.* 2024. № 11. С. 270-274. DOI: https://doi.org/10.32782/2524-0374/2024-11/61

40. Бондар Д.В. Актуальні напрями удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Juris Europensis Scientia*. 2024. № 6. С. 48-53. DOI: https://doi.org/10.32782/chern.v6.2024.9

41. Бондар Д.В. Система принципів, напрямів та способів адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Київський часопис права.* 2024. № 4. С. 40-48. DOI: https://doi.org/10.32782/klj/2024.4.6

42. Бондар Д.В. Адміністративно-правові засади використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності: сучасний стан та напрями удосконалення. *Право і суспільстві.* 2024. № 6. С. 118-125. DOI: https://doi.org/10.32842/2078-3736/2024.6.18

43. Бондар Д.В. Особливості понятійно-категоріального апарату та основні наукові підходи до дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний вісник.* 2024. № 6. С. 30-38. DOI: https://doi.org/10.32782/yuv.v6.2024.4

44. Бондар Д.В. Досвід адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі. *Правові новели.* 2024. № 24. С. 68-76. DOI: https://doi.org/10.32782/ln.2024.24.10

45. Бондар Д.В. Особливості адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в США. *Держава та регіони. Серія: Право.* 2024. № 4. С. 51-58. DOI: https://doi.org/10.32782/1813-338X-2024.4.7

46. Бондар Д.В. Адміністративно-правові засади забезпечення безпеки життєдіяльності та цивільного захисту в Японській Державі в умовах цифровізації. *Право та державне управління.* 2024. № 4. С. 36-45. DOI: https://doi.org/10.32782/pdu.2024.4.5

47. Бондар Д., Бакала В. Протипожежний напрям діяльності національно-культурних товариств на Східній Галичині в 1920–1930-х рр. *Skhidnoievropeiskyi istorychnyi visnyk – East European Historical Bulletin*. 2024. № 33. С. 139-148. DOI: https://doi.org/10.24919/2519-058X.33.317455

48. Бондар Д.В. Особливості адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану. *Науковий вісник Міжнародного гуманітарного університету. Серія: «Юриспруденція».* 2024. № 72. С. 30-35. DOI: https://doi.org/10.32782/2307-1745.2024.72.5

49. Бондар Д.В. Безпека життєдіяльності в умовах інформаційного суспільства: актуальні питання та адміністративно-правові засоби їх вирішення. *Актуальні проблеми вітчизняної юриспруденції.* 2024. № 6. С. 90-97. DOI: https://doi.org/10.32782/2408-9257-2024-6-14

50. Бондар Д.В. Забезпечення безпеки життєдіяльності та цивільний захист: співвідношення понять та особливості адміністративно-правового регулювання. *Науковий вісник публічного та приватного права.* 2024. № 6. С. 35–43. DOI: https://doi.org/10.32844/2618-1258.2024.6.6.

51. Бондар Д.В. Історія становлення та розвитку органів публічної адміністрації у сфері забезпечення безпеки життєдіяльності та цивільного захисту в контексті адміністративно-правового регулювання та цифровізації їх діяльності. *Правова позиція.* 2024. № 4(45). С. 82-89. DOI: https://doi.org/10.32782/2521-6473.2024-4.15

52. Бондар Д.В. Реалізація публічних та приватних інтересів в процесі адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал.* 2024. № 10. С. 654-657. DOI: https://doi.org/10.32782/2524-0374/2024-10/156

53. Бондар Д.В. Цифровізація систем цивільного захисту та забезпечення безпеки життєдіяльності: актуальні питання правового регулювання та матеріально-технічного забезпечення. *Юридичний науковий* електронний журнал. 2024. № 12. С. 543-546. DOI: https://doi.org/10.32782/2524-0374/2024-12/126

54. Бондар Д.В. Адміністративно-правове регулювання захисту персональних даних та інформаційної безпеки у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал.* 2025. № 1. С. 601-605. DOI: https://doi.org/10.32782/2524-0374/2025-1/140

55. Бондар Д.В. Адміністративно-правове регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності. *Право і суспільство.* 2024. № 5. С. 665-672. DOI: https://doi.org/10.32842/2078-3736/2024.5.96

56. Брижко В.М. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція / В.М. Брижко, О.М. Гальченко, В.С. Цимбалюк та ін.; за ред. Р.А. Калюжного та М.Я. Швеця. К.: «Інтеграл», 2002 р. 220 с.

57. Бурбело Б. Інформаційна діяльність суб'єктів забезпечення безпеки дорожнього руху: стан та напрями удосконалення. *Юридична Україна: правовий часопис.* Київський регіональний центр Академії правових наук України; СП «Юрінком Інтер». Київ, 2010. № 7 (91). С. 42-47.

58. Васійчук О.В., Гончарук С.І., Качан С.І., Мохняк С.М. Основи цивільного захисту: навч. посібник. Львів: Вид-во Нац. ун-у «Львівська політехніка», 2010. 417 с.

59. Ватковська М.Г. Досвід Сінгапуру щодо впровадження електронного урядування у сфері освіти. *Збірник наукових праць Донецького держ. ун-ту управління. Сер.: Державне управління.* 2014. Т. 15, Вип. 291. С. 43-51. URL: http://nbuv.gov.ua/UJRN/znpdduu_du_2014_15_291_7

60. Верховна Рада ухвалила закон про зберігання персональних даних українців на закордонних серверах, який є частиною мобілізаційного законодавства. *Судово-юридична газета. Публікації. Законодавство.* 16.01.2024. URL: https://sud.ua/uk/news/publication/290726-verkhovnaya-rada-prinyala-zakon-o-khranenii-personalnykh-dannykh-ukraintsev-na-zarubezhnykh-serverakh-yavlyayuschiysya-chastyu-mobilizatsionnogo-zakonodatelstva (дата звернення: 01.06.2024).

61. Верховний суд Китаю розгляне питання захисту ШІ та інтелектуальної власності. Судово-юридична газета. У світі. 10.03.2025. URL: https://sud.ua/uk/news/abroad/325258-verkhovnyy-sud-kitaya-rassmotrit-vopros-zaschity-ii-i-intellektualnoy-sobstvennosti (дата звернення: 11.03.2025).

62. Веселов М., Забєділіна А. Цивільний захист населення в умовах воєнного стану. *Зовнішня торгівля: економіка, фінанси, право*. 2023. № 4. С. 98-114.

63. Виконання зобов'язань у рамках Угоди про асоціацію. Європейська інтеграція. Міжнародна діяльність. Державна служба України з надзвичайних ситуацій: офіційний веб-сайт. URL: https://dsns.gov.ua/mizhnarona-diyalnist/evropeyska-integraciya (дата звернення: 10.05.2024).

64. Вінник О. Цифровізація в ракурсі державної економіко-правової політики. *Підприємництво, господарство і право.* 2020. № 8. С. 61-70.

65. Вітчизняний і зарубіжний досвід впровадження електронного урядування / Збірник матеріалів науково-практичної конференції; за заг. ред. д-ра наук з держ. упр., проф. С.А. Чукут, канд. наук з держ. упр. О.В. Загвойської. К., 2008. 1128 с.

66. Воловик Л.М., Ковальська К.В., Бондаренко Р.І. Безпека життєдіяльності населення в умовах глобалізації. *Молодий вчений.* 2016. № 9 (1). С. 34-37.

67. Володовська В., Дворовий М. Права людини онлайн: Порядок денний для України. Київ: ГО «Лабораторія цифрової безпеки», 2019. 56 с.

68. Волокіта В. Федоров розповів про впровадження штучного інтелекту в роботу держави. *Економічна правда.* 25.09.2024. URL: https://www.epravda.com.ua/news/2024/09/25/719812/ (дата звернення: 27.09.2024).

69. Воронін А.С. Сучасні проблеми безпеки життєдіяльності. *Нотатки сучасної науки.* 2022. № 3. С. 65-66.

70. Гавловський В., Гриценко В., Цимбалюк В. Організаційно-правові питання формування державної інформаційної політики в Україні. *Науковий вісник. Збірник наукових праць Академії державної податкової служби України.* 2002. № 3 (17). С. 177-182.

71. Галущак О., Галущак М., Машлій Г. Цифровізація в Україні: еволюційні перетворення. *Галицький економічний вісник.* 2023. № 2 (81). С. 155-163.

72. Ганзенко О.О. Теорія правових засобів у контексті інструментальної теорії права. *Вісник Запорізького національного університету: Збірник наукових праць. Юридичні науки.* 2016 № 3. С. 36-42.

73. Ганьба О.Б., Мірошніченко В.І. Особливості сучасної методології правових наукових досліджень. *Парадигма пізнання: гуманітарні питання.* № 2 (13). 2016. С. 1-13.

74. Гастинщиков В. Система народної самооборони Китаю налічує до восьми мільйонів осіб. 03.09.2023. *АРМІЯ INFORM.* URL: https://armyinform.com.ua/2023/09/03/systema-narodnoyi-samooborony-kytayu-nalichuye-do-vosmy-miljoniv-osib/ (дата звернення: 15.09.2024).

75. Глуха В.В., Помаза-Пономаренко А.Л. Нормативно-правове забезпечення державного управління сферою безпеки життєдіяльності. *Державне управління: удосконалення та розвиток.* 2016. № 2. Режим доступу URL: http://nbuv.gov.ua/UJRN/Duur_2016_2_4

76. Говорун С.В. Державне управління у сфері пожежної безпеки Японії: досвід для України. *Науковий вісник: Державне управління.* 2020. № 1 (3). С. 29-52.

77. Голосніченко Д.І. Теорія Повноважень: вітчизняний та зарубіжний досвід їх формування: монографія. К.: Г.А.М., 2009. 356 с.

78. Горденко С.І. Історія виникнення та еволюційний шлях безпеки життєдіяльності. *Переяславський літопис.* 2018. Вип. 13. С. 225-230.

79. Горденко С.І. Основні принципи та методи забезпечення безпеки життєдіяльності людей. *Молодий вчений.* 2016. № 9.1. С. 54-58.

80. Горобцов В.О. Криптографічний захист інформації. Енциклопедія Сучасної України / редкол.: І.М. Дзюба, А.І. Жуковський, М.Г. Железняк та ін.; НАН України, НТШ. К.: Інститут енциклопедичних досліджень НАН України, 2014. Т. 15. URL: https://esu.com.ua/article-1575 (дата звернення: 02.11.2024).

81. Горова С.В. Новітні інформаційні технології в суспільних та культурних процесах сучасної України. *Бібліотекознавство. Документознавство. Інформологія.* 2018. № 1. С. 116-120.

82. Григоренко Н.В. Зарубіжний досвід побудови систем надання державних послуг у сфері цивільного захисту. *Теорія та практика державного управління.* 2015. Вип. 2. С. 290-297. URL: http://nbuv.gov.ua/UJRN/Tpdu_2015_2_47

83. Гринюк Т.О. Безпека людини як комплексний підхід до питань охорони праці, безпеки життєдіяльності, цивільного захисту та пожежної безпеки. *Психолого-педагогічні основи гуманізації навчально-виховного процесу в школі та ВНЗ: зб. наукових праць.* 2013. Вип. 2 (10). С. 38-43.

84. Гришин В.В. Особливості формування єдиного інформаційного простору України на державному рівні. *Наук. вісник Харк. держ. акад. культури.* 2011. Вип. 33. С. 62-69.

85. Грідін К. Урядові програми діджиталізації: досвід ОАЕ та Саудівської Аравії. CFC Big Ideas. URL: https://cfcbigideas.com/uk/uryadovi-programy-didzhytalizacziyi-dosvid-oae-ta-saudivskoyi-araviyi/ (дата звернення: 01.09.2024).

86. Гусарєв С.Д. Юридична діяльність: методологічні та теоретичні аспекти: автореф. дис. на здобуття наук. ступеня д-ра юрид. наук: 12.00.01 «Теорія та історія держави і права; історія політичних і правових вчень». Київ, 2007. 35 с.

87. Доманський В.А. Державне управління пожежною безпекою України (організаційно-правовий аналіз за матеріалами діяльності Державного департаменту пожежної безпеки): дис. … канд. юрид. наук: 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право». К., 2004. 258 с.

88. Данилишин Б.М. Природно-техногенні катастрофи: проблеми економічного аналізу та управління. НАН України; Рада по вивченню продуктивних сил України. К.: ЗАТ «Нічлава», 2001. 259 с.

89. Дашенко Н.М. Інновації у сфері електронного уряду: досвід Китаю. *Міжнародна науково-практична інтернет конференція «Теоретичні та організаційно-методичні засади надання електронних послуг в системі е-урядування».* Одеса: Одеський національний політехнічний університет, 25 квітня 2014 р. С. 48-50. URL: https://economics.net.ua/files/science/e_yrjad/2014/48.pdf

90. Демчук В.В. Реформування сфери цивільного захисту як складової безпекового простору в контексті європейської інтеграції України. *Науковий вісник: державне управління.* 2023. № 1. С. 102-122.

91. Денисова А. Правові засоби: поняття та види. Право України. 2010. № 7. С. 190-195.

92. Денисова А.В. Напрями адміністративного нагляду у сфері забезпечення безпеки життєдіяльності населення: питання систематизації. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2017. Вип. 45 (1). С. 156-159.

93. Денісова О.О. Інформаційні системи і технології в юридичній діяльності: навч. посіб. К.: КНЕУ, 2003. 315 с. URL: http://ukrkniga.org.ua/ukrkniga-text/817/4/

94. Державна служба України з надзвичайних ситуацій. Історія, сучасний стан, основні нормативні акти, коментарі і роз'яснення, методичні та рекомендаційні матеріали для цивільного населення. Київ. ВД «Професіонал», 2022. 510 с.
URL: https://lb.ua/file/company/3573_derzhavna_sluzhba_ukraini_z.html

95. Деякі питання документування управлінської діяльності: Постанова Кабінету Міністрів України від 17 січня 2018 р. № 55. Дата оновлення: 05.07.2024. URL: https://zakon.rada.gov.ua/laws/show/55-2018-п (дата звернення: 01.10.2024).

96. Деякі питання цифрового розвитку: Постанова Кабінету Міністрів України від 30 січня 2019 р. № 56. Дата оновлення: 30.06.2023. URL: https://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF#Text (дата звернення: 01.06.2024).

97. Деякі питання підвищення рівня цифровізації сил безпеки та сил оборони України у період воєнного стану: постанова Кабінету Міністрів України від 04 лютого 2023 р. № 139. URL: https://www.kmu.gov.ua/npas/deiaki-pytannia-pidvyshchennia-rivnia-tsyfrovizatsii-s-a139 (дата звернення: 02.07.2024).

98. Джужа О.М., Орлов Ю.Ю., Калюжний Р.А. Щодо можливості вивчення правових явищ з позицій синергетики. Мего-Інфо – Юридичний портал №1. Теорія держави і права (наукові статті) 2020. URL: http://mego.info/щодо-можливості-вивчення-правових-явищ-з-позицій-синергетики (дата звернення: 02.07.2024).

99. Доронін І.М. Екстраординарний характер реалізації безпекових функцій держави в сучасному світі: інформаційно-правовий аспект. *Інформація і право.* 2018. № 2 (25). С. 85-95.

100. Дубов Д.В., Дубова С.В. Основи електронного урядування. К.: Центр навчальної літератури, 2006. 176 с.

101. Дубов Д., Ожеван М., Баровська А. «Щодо попередження та інформування населення в умовах загрози або виникнення надзвичайної ситуації (на прикладі природної та техногенної катастрофи в Японії)». Аналітична записка. Національний інституту стратегічних досліджень. 12.05.2011. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/schodo-poperedzhennya-ta-informuvannya-naselennya-v-umovakh (дата звернення: 10.10.2024).

102. Дурман М.О., Линецька М.Я. Нормативно-правова база цифрової трансформації українського суспільства. *Діджиталізація та права людини* : збірник тез Міжнародної науково-практичної інтернет-конференції (м. Хмельницький, 30 берез. 2021 р.). Хмельницький: Хмельницький університет управління та права імені Леоніда Юзькова, 2021. С. 124-127.

103. Європейський Союз (ЄС), Рада Європи (РЄ). Співпраця з міжнародними організаціями. Міжнародна діяльність. Державна служба України з надзвичайних ситуацій: офіційний веб-сайт. URL: https://dsns.gov.ua/mizhnarona-diyalnist/spivpracya-z-mizhnarodnimi-organizaciyami/es-ek-re (дата звернення: 10.05.2024).

104. Євсюков О.П. Особливості державного управління в умовах надзвичайних ситуацій. *Актуальні проблеми державного управління.* 2012. № 1. С. 263-267.

105. Єрічева Т.Ю. Становлення та розвиток безпеки життєдіяльності як науки. *Молодий вчений.* 2017. № 9.1. С. 56-59.

106. Єсімов С.С. Методологія дослідження інформаційних технологій у публічному управлінні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2017. Вип. 4. С. 211–221.

107. Єсімов С.С. Використання інформаційних технологій як предмет адміністративно-правового регулювання. *Lviv Polytechnic National University Institutional Repository. Ser.: Ûrid. nauki.* 2015. № 827(8). С. 24-29. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4809/yesimov3.pdf

108. Жарков Я. М., Дзюба М. Т., Замаруєва І. В. Інформаційна безпека особистості, суспільства, держави: підручник. Київ: ВПЦ «Київський університет», 2008. 274 с.

109. Завадська М.М., Осипенко Є.В. Забезпечення безпеки життєдіяльності людини в умовах екстремальних ситуацій. *Молодий вчений.* 2016. № 11 (1). С. 33-36.

110. Загальне адміністративне право: підручник / Гриценко І.С., Мельник Р.С., Пухтецька А.А. та ін.; за заг. ред. І.С. Гриценка. К.: Юрінком Інтер, 2015. 568 с.

111. Заєць О.В. Новітні інформаційні технології як загроза інформаційній безпеці особи. *Форум права.* 2012. № 1. С. 329-333.

112. Заікін А.П. Дігіталізація судової влади: теоретико-правовий аспект: дис. … канд. юрид. наук: 12.00.01 «теорія та історія держави і права; історія політичних і правових учень». Харків, 2021. 197 с.

113. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири : автореф. дис. на здобуття наук. ступеня д-ра політичних наук: 23.00.02 – політичні інститути та процеси. Львів, 2021. 37 с.

114. Захист населення і територій від надзвичайних ситуацій. Т. 1. Техногенна та природна небезпека / за загальною редакцією В.В. Могильниченка. К.: КІМ, 2007. 636 с.

115. Запуск системи автоматичної фіксації порушень Правил дорожнього руху. МВС України. URL: https://mvs.gov.ua/uk/ministry/projekti-mvs/avtofotovideofiksaciya-porusen-pdr/zapusk-sistemi-avtomaticnoyi-fiksaciyi-porusen-pravil-doroznyogo-ruxu-1 (дата звернення: 20.03.2023).

116. Звіт про основні результати діяльності Державної служби України з надзвичайних ситуацій у 2021 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2021/zvit2021-dns.pdf (дата звернення: 07.11.2024).

117. Звіт про основні результати діяльності Державної служби України з надзвичайних ситуацій у 2022 році. URL: https://dsns.gov.ua/upload/1/6/4/9/3/5/0/publicnii-zvit-2022-ostannia-versiia-1.pdf (дата звернення: 07.11.2024).

118. Звіт про основні результати діяльності Державної служби України з надзвичайних ситуацій у 2023 році. URL: https://dsns.gov.ua/upload/2/0/4/5/2/3/6/zvit-pro-osnovni-rezultati-diialnosti-dsns-u-2023-roci.pdf (дата звернення: 07.11.2024).

119. Золотухіна Л.О. Адміністративно-правовий механізм забезпечення реалізації публічного інтересу. *Jurnalul juridic national: teorie şi practică.* 2019. № 4 (38). С. 61-64.

120. Золотухіна Л.О. Діалектика співвідношення публічних і приватних інтересів як адміністративно-правових категорій. *Вісник Запорізького національного університету. Юридичні науки.* 2019. № 1. С. 70-77.

121. Іваненко О. Цифровізація як нова реальність в умовах соціальної нестабільності. *Соціологія: теорія, методи, маркетинг*. 2024. № 3. С. 25-46.

122. Інспектор з охорони праці та техніки безпеки. Профорієнтація. URL: https://osvita.ua/proforientation/profession/75199/ (дата звернення: 08.11.2024).

123. Інтеграція України в Європейське інформаційне суспільство: виклики та завдання: монографія. Київ. ФОП Клименко, 2014. 212 с.

124. Інформаційні технології в юридичній діяльності: навч. посіб. / О.В. Співаковський, М.І. Шерман, В.М. Стратонов, В.В. Лапінський. Херсон: ХДУ, 2012. 220 с.

125. Історія інтернету від ARPANET до сьогодні. 21.11.2019. Ucloud. URL: https://ucloud.ua/istoriya-internetu-vid-arpanet-do-sogodni/ (дата звернення: 02.06.2024).

126. Калашнікова Л.В. Безпека життєдіяльності як предмет соціологічного аналізу: уточнення змісту поняття. *Вісник Одеського національного університету. Соціологія і політичні науки.* 2017. Т. 22. Вип. 1. С. 54-65.

127. Калашнікова Л.В. Особливості вивчення безпеки життєдіяльності як соціального явища. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Соціологічні дослідження сучасного суспільства: методологія, теорія, методи.* 2017. Вип. 39. С. 73-79.

128. Калашнікова Л.В. Співвідношення понять «невизначеність», «ризик», «виклик», «загроза», «небезпека» у контексті соціології безпеки життєдіяльності. *Грані.* 2017. Т. 20. № 5. С. 16-23.

129. Кальман О. Деякі проблеми реформування правоохоронних та контролюючих органів України. *Вісник прокуратури.* 2002. № 4. С. 88-91.

130. Качинський А.Б. Безпека життєдіяльності особи, суспільства та держави: порогові умови. *Стратегічні пріоритети.* 2013. № 2. С. 111-119.

131. Качний О. Законодавчі аспекти впровадження інформаційно-комунікаційних технологій – стратегічного напряму оптимізації державного управління. *Державне управління: удосконалення та розвиток: Електронне наукове фахове видання Дніпропетровського державного аграрно-економічного університету.* 2015. № 5. URL: http://www.dy.nayka.com.ua/?op=1&z=853 (дата звернення: 07.08.2024).

132. Кельман М. Методологія сучасного правознавства: становлення та основні напрями розвитку. *Психологія і суспільство.* 2015. № 4. С. 33-46.

133. Кіберполіція інформує про відповідальність за вчинення різних видів булінгу. Платформа допомоги врятованим. 03.12.2024. URL: https://www.help-platform.in.ua/kiberpolicziya-informuye-pro-vidpovidalnist-za-vchynennya-riznyh-vydiv-bulingu/ (дата звернення: 05.12.2024).

134. Ківалова Т.С., Смелянець Г.Є. До питання про поняття і складові методу правового регулювання. *Актуальні проблеми держави і права.* 2003. Вип. 21. С. 33-38.

135. Кіт Л.Я., Наливайко Н.В. Основи рятування і збереження життя людини, яка перебуває у невідкладному стані: навч. посібник. Львів: ЛНУ імені Івана Франка, 2020. 132 с.

136. Клименко Н. Особливості забезпечення цивільного захисту в умовах воєнного стану. *Науковий вісник: Державне управління.* 2022. № 2 (12). С. 218-233. https://doi.org/10.33269/2618-0065-2022-2(12)-218-233

137. Клімушин П.С. Особливості впровадження світового досвіду електронного врядування із застосуванням портальних технологій. *Державне будівництво.* 2010. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2010_1_43

138. Коваленко В.В., Борисов А.В., Івашина Н.О., Стогній Г.М. Вивчення міжнародного досвіду забезпечення цивільного захисту під час ліквідації наслідків надзвичайних ситуацій. *Науковий вісник: Державне управління*. №1(3) 2020. С. 110-120.

139. Коваль Т.І., Попов М.Д. Застосування інформаційно-комунікаційних технологій у процесі формування компетентності «Безпека життєдіяльності» у майбутніх фахівців. *Теоретичні питання культури, освіти та виховання.* 2017. № 1. С. 98-102.

140. Ковальова Т.В., Гунбіна О.В. Правові проблеми надання адміністративних послуг з використанням інтернет-технологій. *Наукові перспективи. Серія «Право».* 2021. № 9 (15). С. 260-271. URL: http://perspectives.pp.ua/index.php/np/article/download/483/486.

141. Ковжога С.О., Малько О.Д., Полєжаєв А.М. Безпека життєдіяльності: навч. посіб. Х.: Нац. юрид. акад. України, 2010. 224 с.

142. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X. Дата оновлення: 15.04.2023. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 30.04.2023).

143. 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 (дата звернення: 07.11.2024).

144. Кожухар О.Г. Правове регулювання систем штучного інтелекту в ЄС: передумови, сучасний стан та перспективи. *Наукові записки НаУКМА. Юридичні науки.* 2024. Том 13. С. 65-74.

145. Колодій А.М. Принципи права: генеза, поняття, класифікація та реалізація. *Науково-практичний юридичний журнал «Альманах права».* 2012. Вип. 3. С. 42-46.

146. Комаров О.В. Адміністративно-правовий статус суб'єктів здійснення цифрової трансформації регіону. *Юридична наука.* 2020. 12 (114). С. 122-128. URL: https://doi.org/10.32844/2222-5374-2020-114-12.15

147. Коминар Н.М. Інформаційна безпека як складова національної безпеки держави: адміністративно-правовий аспект: дис. … канд. юрид. наук; спец.: 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право». Львів, 2018. 208 с.

148. Конвенція Тромсе як основа цифрового урядування та штучного інтелекту. Національна асоціація адвокатів України. URL: https://unba.org.ua/news/9570-konvenciya-tromse-yak-osnova-cifrovogo-uryaduvannya-ta-shtuchnogo-intelektu.html

149. Конституція України від 28.06.1996. Дата оновлення: 01.01.2020. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 07.11.2024).

150. 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-р#Text (дата звернення: 07.11.2024).

151. Кормич Б.А. Інформаційна безпека: організаційно-правові основи. К.: Кондор, 2004. 384 с.

152. Котерлін І.Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав і свобод. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 1. С. 150-155.

153. Кошель В.І., Сав'юк Г.П., Дзундза Б.С. Безпека життєдіяльності: навчально-методичний посібник. Івано-Франківськ: НАІР, 2018.163 с.

154. Краковська А.Є., Бабик М.К. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2022. Випуск 70. С. 329-334.

155. Кримінальний кодекс України від 05.04.2001 р. № 2341-ІІІ. Дата оновлення: 28.04.2023. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 25.03.2023).

156. Крюков О.І, Махортов П.П., Загинайко В.С., Завада Є.Є. Цивільний захист як наукова категорія в системі національної безпеки. *Вісник Національного університету цивільного захисту України. Серія: Державне управління.* 2023. Вип. 2. С. 437-446.

157. Кузьменко О.В., Чорна В.Г., Островський С.О. Правове регулювання запровадження та використання штучного інтелекту. *Київський часопис права.* 2024. № 1. С. 173-177.

158. Куйбіда В.С., Карпенко О.В., Карпенко О.В., Наместнік В.В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник НАДУ. Серія «Державне управління».* 2018. № 1. С. 5-11.

159. Куракін О.М., Скрябін О.М. Особливості правового регулювання використання штучного інтелекту в Україні. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право».* 2023. Вип. 36. С. 36-42.

160. Курчій Б.О. Енциклопедія безпеки життєдіяльності. Ірпінь: Видавничий центр ВП НУБіП України «ІЕК», 2014. 158 с.

161. Кучма Д.Я. Основні методологічні підходи до дослідження державного механізму забезпечення безпеки життєдіяльності суспільства. *Науково-інформаційний вісник Академії національної безпеки.* 2015. № 1-2. С. 38-67.

162. Кушакова-Костицька Н.В. Методологічні проблеми сучасних правових досліджень: об'єктивна необхідність чи суб'єктивна формальність. *Філософські та методологічні проблеми права.* 2013. № 1-2. С. 23-31.

163. Лавріненко В. Інформаційно-аналітичне забезпечення діяльності органів державної влади. *Вісник Національної академії державного управління при Президентові України.* 2003. №1. С. 502-507.

164. Латишев Є.Є. Безпека здоров'я та життєдіяльності: сучасний стан (за даними аналізу літературних наукових джерел). *Сучасні медичні технології.* 2015. № 2-3. С. 130-135.

165. Лахижа М.І. Діджиталізація в Україні: поняття, проблеми, перспективи та завдання публічного управління. *Науковий вісник: Державне управління.* 2020. № 2(4). С. 202-213.

166. Лещенко О.Я. Міжнародний досвід трансформації систем цивільного захисту в умовах сучасних воєнно-політичних конфліктів. *Молодий вчений («Young Scientist»): науковий журнал.* 2017. Вип. № 8 (48). С. 339-344. URL: http://molodyvcheny.in.ua/files/journal/2017/8/75.pdf (дата звернення: 11.02.2024).

167. Литвиновський Є.Ю., Михайлов В.М., Талан І.С. Організаційно-правові засади діяльності навчально-методичних центрів цивільного захисту та безпеки життєдіяльності. *Науковий збірник Інституту державного управління у сфері цивільного захисту.* 2014. № 2. С. 54-58.

168. Лопушинський І.П. «Цифровізація» як основа державного управління на шляху трансформації та реформування українського суспільства. Теорія та практика державного управління і місцевого самоврядування. 2018. № 2. URL: http://el-zbirn-du.at.ua/2018_2/20.pdf.

169. Лошицький М.В. Адміністративно-правові засоби в механізмі охорони навколишнього середовища. Митна справа. 2015. № 1 (97). С. 79-85.

170. Лук'янова Г.Ю. Методологічні основи дослідження права у сучасній юридичній науці. *Науковий вісник Львівського державного університету внутрішніх справ.* 2011. № 4. С. 33-43.

171. Люблін В.Д., Смілевський М.Л. Правове регулювання відносин в інформаційному середовищі України: адміністративно-правові аспекти: монографія. Львів: Вид-во ЛДУБЖД, 2021. 247 с.

172. Ляшенко В.І., Вишневський О.С. Цифрова модернізація економіки України як можливість проривного розвитку: монографія. НАН України, Інститут економіки промисловості. Київ, 2018. 252 с.

173. Макаренко Л.О. Права і безпека людини в умовах сучасних викликів та загроз. *Альманах права.* 2022. Вип. 13. С. 123-129.

174. Максіменцева Н.О., Максіменцев М.Г., Штучний інтелект у публічному управлінні: переваги цифрових технологій та загрози суверенному інформаційному простору. *Електронний журнал «Державне управління: удосконалення та розвиток».* 2024. № 2. URL: https://www.researchgate.net/publication/378525811_STUCNIJ_INTELEKT_U_PUBLICNOMU_UPRAVLINNI_PEREVAGI_CIFROVIH_TEHNOLOGIJ_TA_ZAGROZI_SUVERENNOMU_INFORMACIJNOMU_PROSTORU

175. Малашко О.Є., Єсімов С.С. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Інтернаука.* 2020. № 14 (94). Т. 2. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/3369/1/%d1%94%d1%81%d1%96%d0%bc%d0%be%d0%b2.pdf

176. Мартин О.М. Захист населення і територій від надзвичайних ситуацій у контексті правового регулювання: досвід країн Заходу. *Організаційно-управлінські, економічні та нормативно-правові аспекти забезпечення діяльності органів управління та підрозділів МНС України. Збірник матеріалів III міжнародної науково-практичної конференції*, м. Черкаси, 15 квітня 2011 року. Черкаси, 2011. С. 187-189.

177. Марченко К.М., Оришака О.В. Інформаційна безпека життєдіяльності людини і суспільства в умовах війни. *Центральноукраїнський науковий вісник. Технічні науки.* 2023. Вип. 7 (1). С. 16-21.

178. Миськовець Н. П. Цифровізація в Україні та світі. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Економіка і управління.* 2019. Т. 30, № 4. С. 63.

179. Місечко В. Закон про штучний інтелект в ЄС: що потрібно знати українцям? Економічна правда. 14.06.2024. URL: https://epravda.com.ua/columns/2024/06/14/715175/ (дата звернення: 02.09.2024).

180. Мороз Є.Д., Близнюк М.Д., Печиборщ В.П., Михайловський М.М., Кушнір В.А., Вороненко В.В. Досвід організації екстреної медичної допомоги потерпілим у надзвичайних ситуаціях у США та розвинених державах світу. Український медичний часопис. 2018. № 4 (126). Т. 2. С. 9-12. URL: https://www.umj.com.ua/article/129631/

181. Мохова Ю.Л. Оцінка діяльності центрів надання адміністративних послуг в умовах цифровізації України. *Публічне управління та митне адміністрування.* 2021. № 2 (29). С. 22–28. URL: http://customs-admin.umsf.in.ua/archive/2021/2/6.pdf.

182. Муравська Ю., Сліпченко Т. Правове регулювання штучного інтелекту в Україні та світі. *Актуальні проблеми правознавства.* 2024. № 1(37). С. 188-195.

183. Мягченко О.П. Безпека життєдіяльності людини та суспільства: навчальний посібник. К., 2008. 286 с.

184. Набув чинності Європейський закон про штучний інтелект. Про основні вимоги та зобов'язання при використанні штучного інтелекту. Міжнародні відносини. Liga zakon. Бізнесу. 08 серпня 2024 р. URL: https://biz.ligazakon.net/analitycs/229699_nabuv-chinnost-vropeyskiy-zakon-pro-shtuchniy-ntelekt-pro-osnovn-vimogi-ta-zobovyazannya-pri-vikoristann-shtuchnogo-ntelektu (дата звернення: 02.09.2024).

185. Наджафлі Е. Розуміння поняття «дигіталізація» в контексті державної влади. *Право і суспільство.* 2021. № 5. С. 201-214.

186. Накази МВС України. Державна служба України з надзвичайних ситуацій. Нормативна база. URL: https://dsns.gov.ua/zakonodavstvo/nakazi-mvs-ukrayini (дата звернення: 17.11.2024).

187. Новий Регламент (ЄС) 2024/1689 від 13 червня 2024 року щодо штучного інтелекту. Пахаренко і партнери: патентно-правова фірма. URL: http://pakharenko.ua/novij-reglament-yes-20241689-vid-13-chervnya-2024-roku-shhodo-shtuchnogo-intelektu/ (дата звернення: 02.09.2024).

188. Обрусна С.Ю., Іванова І.В., Чубань В.С. Проблеми адміністративно-правового забезпечення електронного суду в Україні в умовах пандемії Covid-19. *Юридичний науковий електронний журнал.* 2020. № 4. С. 196-199.

189. Олійник О.В. Адміністративно-правові засоби забезпечення інформаційної безпеки. *Юридичний вісник.* 2015. № 1 (34). С. 65-69.

190. Олійник О.В. Організаційно-правові засади захисту інформаційних ресурсів України: автореф. дис. канд. юрид. наук: спец. 12.00.07 «теорія управління; адміністративне право і процес; фінансове право; інформаційне право». Інститут законодавства Верховної Ради України. Київ, 2006. 22 с.

191. Омельченко А.В. Суспільні відносини у сфері цифровізації як предмет правового регулювання. *Юридична Україна.* 2023. № 10. С. 40-48. DOI 10.37749/2308-9639-2023-10(250)-5

192. Онуфрієнко О.В. Правові засоби у контексті інструментальної теорії права: автореф. дис... канд. юрид. наук: 12.00.01 «теорія та історія держави і права; історія політичних і правових учень»; Національний ун-т внутрішніх справ. Х., 2004. 18 с.

193. Орлов Ю.Ю., Джужа О.М., Орлова О.Ю. Синергетика та пізнання правових явищ. *Науковий вісник Національної академії внутрішніх справ.* 2014. № 1. С. 75-90.

194. Осадчий А.Ю. Цифровізація адміністративних процедур. *Проблеми законності.* 2023. Вип. 163. С. 229-247.

195. Особливості цивільного захисту в умовах воєнного конфлікту: колективна монографія / за ред. Р. Мугаверо, В. Андронова, М. Кустова. Державна служба України з надзвичайних ситуацій. Національний університет цивільного захисту України. Харків – Рим, 2023. 238 с.

196. Остап'юк А.Ю. Досвід США щодо забезпечення цивільного захисту та можливості його використання в Україні. *Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття*: тези доп. учасників VII Всеукр. наук.-практ. конф. (Харків, 9 черв. 2023 р.). Харків: НДІ ППСН, 2023 С. 91–93. URL: https://library.pp-ss.pro/index.php/ndippsn_20230609/article/view/ostapiuk (дата звернення: 15.09.2024).

197. Остапенко О.І. Адміністративно-правова природа безпеки населення України. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* 2021. Випуск 30. С. 234-246.

198. Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки.* 2021. Т. 8. № 3. С. 167-179. URL: http://nbuv.gov.ua/UJRN/vnulpurn_2021_8_3_25

199. Панасюк В.М. Інформатизація та цифровізація: тренди та напрями розвитку в Україні. *Інтелект XXI.* 2020. № 1. С. 160-165.

200. Панфілов В. Система державного правового управління: запобігання техногенно-екологічній небезпеці (законодавча практика США). *Юридичний вісник України.* 1999. 28 жовт. – 3 лист. С. 30-32.

201. Пасмор Ю. В. Цифрові технології як головний чинник економіко-правової модернізації суспільства. *Теорія та практика сучасної юриспруденції: матеріали XXII наук.-практ. конф.*, 15 груд. 2019 р. Харків: ФОП Бровін О.В., 2019. Т. 1. С. 70-72.

202. Пашинський В.Й. Методологічний інструментарій дослідження проблем адміністративно-правового забезпечення оборони держави. *Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право.* 2017. № 3-4. С. 98-102.

203. Переверзєв А.В., Арутюнян В.Е. Інформаційні технології у рішенні задач систем масового оповіщення, перспективи їх вдосконалення та розвитку. *Вісник Криворізького національного університету.* 2019. Вип. 48. С. 46-50.

204. Перун Т.С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. …канд. юрид. наук: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Львів, 2019. 268 с.

205. Петренко Н.О., Машковська Л.О. Цифровізація державних адміністративних послуг в Україні: нормативно-правові аспекти. *Розбудова держави і права: питання теорії та конституційної практики.* 2020. № 2. С. 112-119. URL: http://pravoisuspilstvo.org.ua/archive/2020/2_2020/part_1/20.pdf.

206. Пилипчук В.Г. Становлення і розвиток інформаційного суспільства в Україні: особливості, проблеми, правове регулювання. *Теоретико-правові основи формування та розвитку інформаційного суспільства: матеріали науково-практичної конференції* (м. Київ, 29 лист. 2017 р.) / упоряд. В.М. Фурашев, С.Ю. Петряєв. Київ: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. С. 7-11.

207. Пилипчук В.Г., Брижко В.М. Трансформація системи захисту персональних даних та приватності в контексті євроінтеграції України. *Вісник Національної академії правових наук України.* 2017. № 3(90). С. 36-50.

208. Пилипчук В.Г., Цимбалюк В.С. Історико-правові проблеми становлення і розвитку інформаційної сфери та інформаційного права в Україні (кінець XX – початок XXI століття). *Вісник Національної академії правових наук України.* 2016. № 4 (87). С. 29-44.

209. Питання Міністерства цифрової трансформації: постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856. Дата оновлення: 01.06.2024. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text (дата звернення: 07.11.2024).

210. Пищикова О.В., Сахно С.І., Янова Л.О. Освітленість і безпека життєдіяльності і праці людини. *Вісник Криворізького національного університету.* 2012. Вип. 30. С. 79-84.

211. Підсумки 2022 року в напрямі цифровізації ДСНС України. ДСНС України: офіційний веб-сайт. URL: https://dsns.gov.ua/news/ostanni-novini/pidsumki-2022-roku-v-napriami-cifrovizaciyi-dsns-ukrayini (дата звернення: 12.11.2024).

212. Платні послуги ДВГРЗ ДСНС України. Державний воєнізований гірничорятувальний загін. URL: https://dvgrz.dsns.gov.ua/poslugi-dvgrz-dsns-ukrayini (дата звернення: 12.12.2024).

213. Плескач В.Л., Затонацька Т.Г. Інформаційні системи і технології на підприємствах: підручник. К.: Знання, 2011. 718 с. URL: https://drive.google.com/file/d/1KHaGifyfcHmwHhNV89WWCI93eJQsjAiF/view

214. Погребняк В.Я. Синергетичний підхід у методології дослідження механізму переходу цивільних прав та обов'язків. *Актуальні проблеми вітчизняної юриспруденції.* 2017. № 1. № 6. Т. 1. С. 70-73.

215. Погребняк С.П. Основоположні принципи права (змістовна характеристика): монографія. Х.: Право, 2008. 240 с.

216. Подобєд І.В. Цифровізація як сучасний тренд трансформації ресурсного механізму системи цивільного захисту. *Науковий вісник: державне управління.* 2024. № 1. С. 82-103.

217. Подскальна О.А. Приєднання України до механізму цивільного захисту Європейського Союзу – один із пріоритетів її європейського вибору. *Інвестиції: практика та досвід.* 2015. № 19. С. 130-134.

218. Позова Д.Д. Перспективи правового регулювання штучного інтелекту за законодавством ЄС. *Часопис цивілістики.* 2017. Вип. 27. С. 116-120.

219. Полежаєв А.М., Ковжога С.О., Карманний Є.В., Малько О.Д.. Особливості системи «Безпека життєдіяльності людини» як об'єкта управління. *Системи обробки інформації.* 2012. Вип. 3 (2). С. 245-247.

220. Положення про Державну службу України з безпеки на транспорті: затверджене постановою Кабінету Міністрів України від 11.02.2015 № 103. Дата оновлення: 03.05.2023. URL: https://zakon.rada.gov.ua/laws/show/103-2015-п#Text (дата звернення: 02.06.2023).

221. 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-п#Text (дата звернення: 07.11.2024).

222. Положення про Міністерство цифрової трансформації України, затверджене 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 (дата звернення: 07.11.2024).

223. Положення про службу безпеки дорожнього руху Державної служби України з надзвичайних ситуацій, затверджене наказом МВС України 18.09.2018 № 764. Дата оновлення: 30.10.2018. URL: https://zakon.rada.gov.ua/laws/show/z1121-18#Text (дата звернення: 02.06.2023).

224. Положення про службу безпеки дорожнього руху міністерств, інших центральних органів державної виконавчої влади, підприємств, їх об'єднань, установ і організацій, затверджене постановою Кабінету Міністрів України від 05.04.1994 № 227. Дата оновлення: 21.09.2018. URL: https://zakon.rada.gov.ua/laws/show/227-94-п#Text (дата звернення: 02.06.2023).

225. Порядок утворення та функціонування пожежно-рятувальних підрозділів для забезпечення добровільної пожежної охорони: постанова Кабінету Міністрів України №314 від 07.04.2023. Дата оновлення: 12.04.2023. URL: https://zakon.rada.gov.ua/laws/show/314-2023-п#Text (дата звернення: 25.05.2023).

226. Порядок утворення та функціонування пожежно-рятувальних підрозділів для забезпечення місцевої пожежної охорони: постанова Кабінету Міністрів України №315 від 07.04.2023. Дата оновлення: 12.04.2023. URL: https://zakon.rada.gov.ua/laws/show/315-2023-п#Text (дата звернення: 25.05.2023).

227. Пояснювальна записка до проекту Закону України «Про добровільну пожежну охорону» від 15.07.2016 № 4011a. Liga zakon. URL: https://ips.ligazakon.net/document/GH33F68A?an=4 (дата звернення: 17.11.2024).

228. Правові засоби стимулювання інноваційного розвитку України в умовах євроінтеграції: монографія / О.П. Подцерковний, М.Д. Василенко, Д.В. Зятіна, Л.Д. Романадзе та ін.; за заг. ред. С.В. Ківалова, О.П. Подцерковного. Одеса: Фенікс, 2015. 270 с.

229. Працівникам державних органів та військовослужбовцям заборонили користуватися Telegram – РНБО. Судово-юридична газета. Публікації. 20.09.2024. URL: https://sud.ua/uk/news/publication/311056-rabotnikam-gosudarstvennykh-organov-i-voennosluzhaschim-zapretili-polzovatsya-telegram-snbo (дата звернення: 21.09.2024).

230. Присяжнюк М., Бєлошевич Я. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.* 2013. Вип. 30. С. 42-46.

231. Приходько Р.В. Сучасний стан структури органів державного управління у сфері протидії виникненню і ліквідації надзвичайних ситуацій. *Актуальні проблеми державного управління.* 2011. № 1. С. 211-218.

232. Приходько Р., Ященко О. Закордонний досвід регулювання запобігання і ліквідації надзвичайних ситуацій на регіональному рівні. Вісник Національного університету цивільного захисту України. Серія: Державне управління. 2016. Вип. 2. С. 272-282.

233. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України 23 лютого 2006 р. № 3475-IV. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 01.07.2024).

234. Про дорожній рух: Закон України від 30.06.1993 № 3353-XII. Дата оновлення: 23.03.2023 URL: https://zakon.rada.gov.ua/laws/show/3353-12/ed20230323#Text (дата звернення: 05.04.2023)

235. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. Дата оновлення: 01.01.2023. URL: http://zakon2.rada.gov.ua/laws/show/2939-17. (дата звернення: 01.04.2023).

236. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки: розпорядження Кабінету Міністрів України від 9 травня 2025 р. № 457-р. Дата оновлення: 09.05.2025. URL: https://zakon.rada.gov.ua/laws/show/457-2025-р#Text (дата звернення: 10.05.2025).

237. Про затвердження Правил пожежної безпеки в Україні: наказ МВС України від 30 грудня 2014 № 1417. Дата оновлення: 14.08.2024. URL: https://zakon.rada.gov.ua/laws/show/z0252-15#Text (дата звернення: 15.12.2024).

238. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. № 851-IV. Дата оновлення: 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 01.06.2024).

239. Про електронні комунікації: Закон України від 16 грудня 2020 р. № 1089-IX. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 01.06.2024).

240. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 2155-VIII. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 01.11.2024).

241. Про запобігання корупції: Закон України від 14 жовтня 2014 р. № 1700-VII. Дата оновлення: 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/1700-18 (дата звернення: 05.02.2023).

242. Про затвердження Державної програми підвищення рівня безпеки дорожнього руху в Україні на період до 2023 р.: постанова Кабінету Міністрів України № 1287 від 21.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1287-2020-%D0%BF#Text (дата звернення: 03.06.2024).

243. Про затвердження Інструкції про порядок взаємодії між Державною службою України з надзвичайних ситуацій, Національною поліцією України та Національною гвардією України у сфері запобігання і реагування на надзвичайні ситуації, пожежі та небезпечні події: наказ МВС України від 22 серпня 2016 р. за № 859. Дата оновлення: 07.10.2016. URL: https://zakon.rada.gov.ua/laws/show/z1254-16#Text (дата звернення: 07.11.2024).

244. Про затвердження Плану реагування на надзвичайні ситуації державного рівня: постанова Кабінету Міністрів України від 14 березня 2018 р. № 223. Дата оновлення: 03.05.2023. URL: https://zakon.rada.gov.ua/laws/show/223-2018-п#Text (дата звернення: 05.10.2024).

245. Про затвердження Положення про Державну службу України з безпеки на транспорті: постанова Кабінету Міністрів України від 11 лютого 2015 р. № 103. Дата оновлення: 12.09.2024. URL: https://zakon.rada.gov.ua/laws/show/103-2015-п#Text (дата звернення: 08.11.2024).

246. Про затвердження Положення про Державну службу України з надзвичайних ситуацій: постанова Кабінету Міністрів України від 16 грудня 2015 р. № 1052. Дата оновлення: 17.08.2024. URL: https://zakon.rada.gov.ua/laws/show/1052-2015-п#Text (дата звернення: 07.11.2024).

247. Про затвердження Положення про Державну службу України з питань безпечності харчових продуктів та захисту споживачів: постанова Кабінету Міністрів України від 2 вересня 2015 р. № 667. Дата оновлення: 16.02.2022. URL: https://zakon.rada.gov.ua/laws/show/667-2015-п#Text (дата звернення: 08.11.2024).

248. Про затвердження Положення про Державну службу України з питань праці: постанова Кабінету Міністрів України від 11 лютого 2015 р. № 96. Дата оновлення: 05.01.2024. URL: https://zakon.rada.gov.ua/laws/show/96-2015-п#Text (дата звернення: 08.11.2024).

249. Про затвердження Положення про єдину державну систему цивільного захисту: постанова Кабінету Міністрів України від 9 січня 2014 р. №11. Дата оновлення: 17.08.2024. URL: https://zakon.rada.gov.ua/laws/show/11-2014-п#Text (дата звернення: 07.11.2024).

250. 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 (дата звернення: 07.11.2024).

251. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141. Дата оновлення: 01.01.2022. URL: https://zakon.rada.gov.ua/laws/show/z0862-07#Text (дата звернення: 02.11.2024).

252. Про затвердження положень про самостійні структурні підрозділи апарату ДСНС та підрозділи у їх складі: Наказ ДСНС № 277 від 30 квітня 2020 р. URL: https://www.dsns.gov.ua/files/2020/6/23/3/277-30.04.2020.pdf (дата звернення: 02.11.2024).

253. Про затвердження Положення про службу безпеки дорожнього руху міністерств, інших центральних органів державної виконавчої влади, підприємств, їх об'єднань, установ і організацій: постанова Кабінету Міністрів України від 5 квітня 1994 р. № 227. Дата оновлення: 21.09.2018. URL: https://zakon.rada.gov.ua/laws/show/227-94-%D0%BF#Text (дата звернення: 08.11.2024).

254. Про затвердження Положення про підсистему реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт єдиної державної системи цивільного захисту: наказ МВС України № 356 від 04 травня 2016 р. URL: https://zakon.rada.gov.ua/laws/show/z0792-16#Tex (дата звернення: 05.01.2025).

255. Про затвердження Положення про функціональну підсистему «Система управління силами та засобами цивільного захисту» єдиної інформаційної системи Міністерства внутрішніх справ: наказ Міністерства внутрішніх справ України від 20.04.2023 № 326. URL: https://iplex360.com.ua/npa.php?doc=1237.1552.0 (дата звернення: 07.11.2024).

256. Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями: постанова Кабінету Міністрів України від 24 березня 2004 р. № 368. Дата оновлення: 31.12.2021. URL: https://zakon.rada.gov.ua/laws/show/368-2004-п#Text (дата звернення: 07.11.2024).

257. Про затвердження Статуту дій у надзвичайних ситуаціях органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту та Статуту дій органів управління та підрозділів Оперативно-рятувальної служби цивільного захисту під час гасіння пожеж: наказ МВС України № 340 від 26.04.2018. Дата оновлення: 18.04.2024. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/RE32253.html (дата звернення: 07.11.2024).

258. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр?find=1&text=крипто#w1_1 (дата звернення: 02.11.2024).

259. Про захист людини від впливу іонізуючого випромінювання: Закон України від 14 січня 1998 р. № 15/98-ВР. Дата оновлення: 17.09.2023. URL: https://zakon.rada.gov.ua/laws/show/15/98-вр#Text (дата звернення: 25.12.2024).

260. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 27.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17/ed20240427#Text (дата звернення: 07.11.2024).

261. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. Дата оновлення: 27.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 01.11.2024).

262. 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. Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/284/99#Text (дата звернення: 07.11.2024).

263. Про Національний координаційний центр кібербезпеки: Указ Президента України від 7 червня 2016 р. № 242/2016. Дата оновлення: 17.07.2021. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 01.07.2024).

264. Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII. Дата оновлення: 16.08.2024. URL: ttps://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 12.12.2024).

265. Про Національну програму інформатизації: Закон України від 1 грудня 2022 р. № 2807-IX. Дата оновлення: 01.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2807-20#n191 (дата звернення: 01.06.2024).

266. Про мобілізаційну підготовку та мобілізацію: Закон України від 21 жовтня 1993 р. № 3543-XII. Дата оновлення: 01.01.2025. URL: https://zakon.rada.gov.ua/laws/show/3543-12#Text (дата звернення: 10.02.2025).

267. Про невідкладні заходи із забезпечення безпеки дорожнього руху: Указ Президента України від 20.11.2007 р. № 1121/2007. Дата оновлення: 25.06.2008. https://zakon.rada.gov.ua/laws/show/1121/2007#Text (дата звернення: 15.02.2023).

268. Про обов’язковий примірник документів: Закон України від 9 квітня 1999 року № 595-XIV. Дата оновлення: 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/595-14#Text (дата звернення: 02.01.2025).

269. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 02.11.2024).

270. Про основні принципи та вимоги до безпечності та якості харчових продуктів: Закон України від 3 грудня 1997 р. № 771/97-ВР. Дата оновлення: 18.12.2024. URL: https://zakon.rada.gov.ua/laws/show/771/97-вр#Text (дата звернення: 08.11.2024).

271. Про охорону праці: Закон України від 4 жовтня 1992 р. № 2694-XII. Дата оновлення: 15.11.2024. URL: ttps://zakon.rada.gov.ua/laws/show/2694-12/ed20241115#Text (дата звернення: 17.11.2024).

272. Про Правила дорожнього руху: Постанова Кабінету Міністрів України № 1306 від 10.10.2001. Дата оновлення: 01.11.2021. URL: https://zakon.rada.gov.ua/laws/show/1306-2001-п/ed20211101#Text (дата звернення: 12.01.2022).

273. Про правовий режим надзвичайного стану: Закон України від 16 березня 2000 р. № 1550-III. Дата оновлення: 18.05.2024. URL: https://zakon.rada.gov.ua/laws/show/1550-14#Text (дата звернення: 07.11.2024).

274. Про правовий режим воєнного стану: Закон України від 12 травня 2015 р. № 389-VIII. Дата оновлення: 08.02.2025. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 10.02.2025)

275. Про ратифікацію Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027): Закон України від 23 лютого 2023 р. № 2926-IX. Дата оновлення: 01.04.2023. URL: https://zakon.rada.gov.ua/laws/show/2926-20#Text (дата звернення: 01.06.2024).

276. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. Дата оновлення: 28.08.2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 02.11.2024).

277. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 р. № 685/2021. Дата оновлення: 30.12.2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 02.11.2024).

278. Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15 липня 2021 р. № 1667-IX. Дата оновлення: 01.01.2023. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text (дата звернення: 01.06.2024).

279. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL: https://www.kmu.gov.ua/npas/250287124 (дата звернення: 01.10.2024).

280. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації: Розпорядження Кабінету Міністрів України від 3 березня 2021 р. № 167-р. Дата оновлення: 03.03.2021. URL: https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text (дата звернення: 01.06.2024).

281. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження КМУ від 2 грудня 2020 р. № 1556-р. Дата оновлення: 29.12.2021. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 12.01.2022).

282. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 листопада 2021 р. № 1467-р. Дата оновлення: 11.04.2023. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#Text (дата звернення: 01.06.2024).

283. Про схвалення Стратегії підвищення рівня безпеки дорожнього руху в Україні на період до 2024 року: розпорядження Кабінету Міністрів України від 21.10.2020. № 1360-р. URL: https://zakon.rada.gov.ua/laws/show/1360-2020-%D1%80#Text (дата звернення: 21.03.2023).

284. Про схвалення Стратегії розвитку вищої освіти в Україні на 2022-2032 роки: розпорядження Кабінету Міністрів України від 23 лютого 2022 р. № 286-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-strategiyi-rozvitku-vishchoyi-osviti-v-ukrayini-na-20222032-roki-286- (дата звернення: 05.04.2024).

285. Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року: розпорядження Кабінету Міністрів України від 10 липня 2019 р. № 526-р. Дата оновлення: 10.07.2019. URL: https://zakon.rada.gov.ua/laws/show/526-2019-р#Text (дата звернення: 12.12.2024).

286. Про схвалення Стратегії цифрової трансформації соціальної сфери: Розпорядження Кабінету Міністрів України від 28 жовтня 2020 р. № 1353-р. URL: https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text (дата звернення: 01.06.2024).

287. Про утворення Координаційної ради з безпеки дорожнього руху: постанова Кабінету Міністрів України від 28.02.2018 р. № 153 URL: https://zakon.rada.gov.ua/laws/show/153-2018-%D0%BF#Text (дата звернення: 15.02.2023).

288. Про цифровий контент та цифрові послуги: Закон України від 10 серпня 2023 р. № 3321-IX. Дата оновлення: 02.03.2024. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text (дата звернення: 01.06.2024).

289. Проект Закону про внесення змін до Кримінального процесуального кодексу України та Закону України «Про запобігання та протидію домашньому насильству» щодо встановлення відповідальності за злочинне переслідування (сталкінг). Картка законопроекту. Пояснювальна записка. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/44972 (дата звернення: 05.10.2024).

290. Проєкт Закону України «Про цифровий порядок денний України». Офіційний веб-сайт Верховної Ради України. URL: https://www.rada.gov.ua/uploads/documents/40009.pdf (дата звернення: 12.12.2024).

291. Прощин І. Аналіз закордонного досвіду із запобігання та ліквідації наслідків надзвичайних ситуацій природного характеру. Збірник наукових праць Черкаського інституту пожежної безпеки імені Героїв Чорнобиля Національного університету цивільного захисту України «Надзвичайні ситуації: попередження та ліквідація». 2021. № 2. Т. 5. С. 95-100.

292. Психолого-педагогічні основи гуманізації навчально-виховного процесу в школі та ВНЗ: зб. наук. праць / ред. кол.: А.С. Дем’янчук, В.І. Борейко, Й.В. Джунь та ін.; Міжнар. економ-гуманіт. ун. ім. акад. Степана Дем’янчука. Рівне: РВЦ МЕГУ ім. акад. С. Дем’янчука, 2013. Вип. 2(10). С. 38-43.

293. Рабінович П.М. Методологія юридичної науки. Юридична енциклопедія: в 6 т. / голова редкол. Ю.С. Шемшученко. К.: Вид-во Українська енциклопедія імені М. П Бажана, 1998-2004. Т. 3: К-М. 2001. 789 с.

294. Радиш Я.Ф. Досвід взаємодії міжнародних цивільно-військових сил при ліквідації наслідків надзвичайних ситуацій. *Держава та регіони.* 2009. № 2. С. 157-160.

295. Руденко І., Полукаров Ю. Досвід Федеративної Республіки Німеччини з організації системи цивільного захисту. *Проблеми охорони праці, промислової та цивільної безпеки.* 2019. С. 370-378.

296. Сергій Тюрін провів нараду щодо впровадження системи «Я – Доброволець». Хмельницька обласна військова адміністрація. Офіційне інтернет-представництво. Новини. 15.08.2024. URL: https://www.adm-km.gov.ua/?p=143081#:~:text=Як%20зауважив%20Сергій%20Тюрін%20на,свій%20професійний%20досвід%20і%20навички. (дата звернення: 07.11.2024).

297. Смілевський М.Л. Щодо необхідності використання світового досвіду правового регулювання відносин в інформаційній сфері. Форум права. № 3. 2012. URL: http://www.nbuv.gov.ua/ejournals/FP/2012-3/12smlvic.pdf

298. Снопок О. Як Верховний суд США поступово стає регулятором у сфері соціальних мереж. Опора. Tech. 10.03.2023. URL: https://www.oporaua.org/polit_ad/iak-verkhovnii-sud-ssha-postupovo-staie-reguliatorom-u-sferi-sotsialnikh-merezh-24609 (дата звернення: 02.06.2024).

299. Сопілко І. М. Методологічні засади виокремлення інформаційного права в системі права України. *Повітряне і космічне право: юридичний вісник.* 2011. № 1 (18). С. 46-50.

300. Сопілко І.М., Череватюк В.Б. Безпека людини в сучасних умовах: загрози та правові шляхи їх вирішення. *Юридичний вісник. Повітряне і космічне право.* 2017. № 1. С. 189-193.

301. Сохін О. Взаємодія рятувальних служб США. *Надзвичайна ситуація.* 2000. № 3. С. 31-32.

302. Співак О.М. Правові засади регулювання штучного інтелекту в Україні та Польщі. *Юридичний науковий електронний журнал.* 2024. № 4. С. 815-817.

303. Степаненко В.П. Інформаційне суспільство. Енциклопедія Сучасної України / редкол.: І.М. Дзюба, А.І. Жуковський, М.Г. Железняк та ін.; НАН України, НТШ. К.: Інститут енциклопедичних досліджень НАН України, 2011. URL: https://esu.com.ua/article-12462 (дата звернення: 08.11.2024).

304. Степанов В.Ю. Цифровізація та ризики цифрової безпеки. *Вісник Національного університету цивільного захисту України. Серія: Державне управління.* 2024. Вип. 1. С. 55-61.

305. Стефанчук Р. Інформаційні технології та право: quo vadis? *Право України.* 2018. № 1. С. 30-50.

306. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. Дата оновлення: 07.01.2025.
URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 19.01.2025).

307. Сяська О.В., Поліщук О.Ю., Савченко О.Р. Нові інформаційні технології в публічному управлінні: проблеми та перспективи. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування.* 2024. № 1. Том 35 (74). С. 157-163. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2024/1_2024/29.pdf

308. Терент'єва А. Досвід Держави Ізраїль щодо управління безпекою цивільного населення в умовах кризових ситуацій. *Науковий вісник: Державне управління.* 2023. № 2 (14). С. 310-333.

309. Терехов В.Ю. Теоретичні аспекти розуміння категорій «безпека людини» та «громадська безпека». *Соціологія права.* 2017. № 1-2. С. 95-101.

310. Тихий В.П. Безпека людини – головний об’єкт національної безпеки України. *Духовність особистості: методологія, теорія і практика.* 2017. Вип. 4. С. 323-329.

311. Тихомиров Д. Наукові методологічні підходи під час дослідження державної політики у сфері безпеки. *Підприємництво, господарство і право.* 2020. № 3. С. 230-234.

312. Тищенкова І.О. Адміністративні процедури надання електронних публічних послуг публічною адміністрацією в Україні. *Форум права. Юридичний форум.* 2017. № 2. С. 124-129. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/FP_index.htm_2017_2_21.pdf

313. Ткачук К.Н., Зеркалов Д.В. Охорона праці та безпека життєдіяльності у концепції розвитку людини. *Проблеми охорони праці в Україні*. 2013. Вип. 26. С. 32-44.

314. Ткачук Р.Л. Інформаційні технології формування прийняття цільових рішень для ліквідації надзвичайних ситуацій в потенційно небезпечних об'єктах виробничих систем. *Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова.* 2013. Вип. 69. С. 209-221.

315. Труш О.О. Досвід побудови та функціонування систем цивільного захисту країн-членів ЄС Західної Європи. *Теорія та практика державного управління.* 2009. Вип. 4. С. 364-373. URL: http://nbuv.gov.ua/UJRN/Tpdu_2009_4_54 (дата звернення: 11.02.2024).

316. Уварова О.О. Принципи права у правозастосуванні: загальнотеоретична характеристика: монографія. Харків: «Друкарня МАДРИД», 2012. 196 с.

317. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, ратифікована із заявою Законом України № 1678-VII від 16.09.2014. Дата оновлення: 30.11.2023. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 07.11.2024).

318. Україна приєдналася до програми Європейського Союзу «Цифрова Європа» (2021 – 2027). Вища школа адвокатури НААУ. URL: https://www.hsa.org.ua/blog/ukrayina-prijednalasia-do-programi-jevropeiskogo-soiuzu-cifrova-jevropa-2021-2027 (дата звернення: 01.06.2024).

319. Ушакова І.О., Плеханова Г.О. Інформаційні системи та технології на підприємстві: конспект лекцій. Харків: Вид. ХНЕУ, 2009.128 с.

320. Федотова О.О. Інформаційна політика ЄС із забезпечення безпеки діяльності користувачів в інтернет-середовищі. *Матеріали ІІІ Міжнародної науково-практичної конференції «Прикладні аспекти сучасних міждисциплінарних досліджень»* (м. Вінниця, 1 листопада 2024 р.). ДонНУ ім. Василя Стуса. С. 84-86. URL: https://jpasmd.donnu.edu.ua/article/view/16716 (дата звернення: 12.11.2024).

321. Фіалка М.І. Використання технічних засобів контролю за безпекою дорожнього руху як напрямок ранньої профілактики злочинів у сфері дотримання правил дорожнього руху. *Державна політика у сфері убезпечення дорожнього руху: теорія, законодавство, практика* : матеріали Всеукр. наук.-практ. конф. (м. Харків, 5 листоп. 2021 р.). НДІ вивч. проблем злочинності ім. акад. В.В. Сташиса НАПрН України. Харків: Право, 2021. С. 118-121.

322. Філіпченко А.С. Адміністративно-правове регулювання захисту населення і територій від надзвичайних ситуацій техногенного та природного характеру: автореф. дис… канд. юрид. наук: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право; НУДПС України. К., 2008. 20 с.

323. Фоменко А.Є., Грибан В.Г. Цивільний захист в Україні: створення та функціонування. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2022. № 1. С. 7-14.

324. Халмурадов Б.Д., Глива В.А. Вступ до фаху: навч. посіб. для студентів за напрямом підготовки «Цивільна безпека». Київ: Центр учбової літератури, 2015. 200 с.

325. Харченко Н.П. Правовий режим: окремі загальнотеоретичні аспекти. *Науковий вісник Херсонського державного університету. Серія Юридичні науки.* 2016. Випуск 2. Том 1. С. 32-35.

326. Хитра О.Л. Особливості діяльності Державної служби з надзвичайних ситуацій щодо реалізації державної політики у сфері цивільного захисту населення. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* 2022. Випуск 32. С. 212-219.

327. «Цифрова Україна»: конституційно-правова модель / Р.О. Стефанчук та ін.; заг. ред.: Р.О. Стефанчук та ін.; Ін-т законодавства Верхов. Ради України. Київ: Ін-т законодавства Верхов. Ради України, 2021. 687 с.

328. Цифрова стратегія ЄС. Проєкти EU4Digital. URL: https://eufordigital.eu/uk/discover-eu/eu-digital-strategy/ (дата звернення: 02.09.2024).

329. Цифрова трансформація публічного управління: колект. монографія / О.В. Карпенко та ін.; Нац. акад. держ. упр. при Президентові України. Київ: НАДУ, 2020. 254 с.

330. Цифрове врядування: монографія / О.В. Карпенко та ін.; за ред. д-ра наук з держ. упр., доц. Карпенка Олександра Валентиновича; Нац. акад. держ. упр. при Президентові України, Каф. інформ. політики та цифр. технологій. Київ: Ідея Принт, 2020. 336 с.

331. Цифровізація та Розумні технології. Агенція Європейських Інновацій. URL: https://aei.org.ua/cyfryzaciya-ta-smart-tehnologii/ (дата звернення: 05.01.2025).

332. Чекригін О.М. Принципи діяльності державної служби України з надзвичайних ситуацій із запобігання надзвичайним ситуаціям. *Юридичний науковий електронний журнал.* 2023. № 2. С. 637-641.

333. Чорноус А. Механізм адміністративно-правового регулювання національної інформаційної інфраструктури України: монографія; Київ. нац. ун-т ім. Тараса Шевченка. Львів; Торунь: Ліга-Пресс, 2021. 211 с.

334. Чукут С.А. Зарубіжний досвід упровадження електронного урядування / Камінська Т., Каменський А., Пасічник М. та ін.; за заг. ред. д-ра наук з держ. упр., проф. С.А. Чукут К., 2008. 200 с.

335. Чукут С. Сутність електронного уряду та принципи його організації. *Вісник Національної академії державного управління при Президентові України.* 2003. №2. С. 429-433.

336. Шатіло В. Принципи діяльності державної влади і методи їх здійснення. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки.* 2014. Вип. № 1. С. 66-70.

337. Швець М., Калюжний Р., Гавловський В., Цимбалюк В. Інформаційне законодавство України: концептуальні основи формування. *Право України.* 2001. № 7. С. 88-91.

338. Шевченко Б.О., Непокупна Т.А., Лашко Т.Б. Капітал безпеки життєдіяльності суспільства, його сутність, структура, сфери застосування: від індивіда до територіальної громади та держави. *Ефективна економіка.* 2022. № 12. Режим доступу URL: http://nbuv.gov.ua/UJRN/efek_2022_12_46

339. Шемелін Д.А. Диспозитивність в адміністративному праві – нові ознаки методу правового регулювання. *Форум права.* 2008. № 1. С. 453-458.

340. Шойко В.А. Європейський досвід формування організаційного забезпечення механізмів державного управління у сфері цивільного захисту. *Актуальні проблеми державного управління.* 2020. № 1 (57). С. 253-260.

341. Шпекторенко І.В. Методологія публічного управління. навч. посіб. Дніпро: ДРІДУ НАДУ. 2018. 120 с.

342. Штучний інтелект, «розумні» алгоритми та роботизація – 20 готових застосунків на Creatio Marketplace. *Terrasoft.* 19.03.2021. URL: https://www.terrasoft.ua/business/news/66367 (дата звернення: 07.01.2025).

343. Шумейко О.А. Зарубіжний досвід забезпечення безпеки дорожнього руху за допомогою автоматизованих систем (на прикладі деяких країн Європи та США). *Науковий вісник публічного та приватного права.* 2016. Випуск 6. Том. 2. С. 77-82.

344. Шумейко Т.А. Адміністративно-правове регулювання безпеки дорожнього руху за допомогою автоматизованих систем: дис. … канд. юрид. наук: 12.00.07 «адміністративне право і процес; фінансове право; інформаційне право»; Відкритий міжнародний університет розвитку людини «Україна». Київ, 2017. 220 с.

345. Шумейко О. Поняття та зміст адміністративно-правового регулювання дорожнього руху за допомогою автоматизованих систем. *Підприємництво, господарство і право.* 2017. № 2. С. 172-177.

346. Юровська В. Метод адміністративного права: теоретико-правовий аналіз. *Підприємництво. господарство і право.* 2017. № 12. С. 188-192.

347. Юровська В.В. Імперативний метод адміністративного права: окремі думки щодо подальших перспектив дослідження. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2017. Випуск 3/4 (35/36). С. 151-154.

348. Юровська В.В. Класифікація методів адміністративного права: критерії та види. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція.* 2017. Вип. 29 (1). С. 59-63. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2017_29%281%29__17

349. «Я – доброволець»: в Україні презентували концепцію інноваційної безпекової платформи. Міністерство внутрішніх справ України. Пресцентр. Новини. URL: https://mvs.gov.ua/news/ia-dobrovolec-v-ukrayini-prezentuvali-koncepciiu-innovaciinoyi-bezpekovoyi-platformi (дата звернення: 07.11.2024).

350. Як штучний інтелект використовується у сфері відкритих даних? Портал «Дія». URL: https://diia.data.gov.ua/info-center/aiod (дата звернення: 07.11.2024).

351. A Digital Single Market Strategy for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2015. EUR-Lex. European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192 (дата звернення: 01.11.2024).

352. Bondar D.A. The system of entities using information technologies in the field of life safety: administrative, legal and economic principles of effective functioning. *Baltic Journal of Economic Studies*. 2024. Vol. 10. № 5. P. 131-136. DOI: https://doi.org/10.30525/2256-0742/2024-10-5-131-136

353. Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions «Shaping Europe's digital future». Brussels, 19.02.2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:67:FIN

354. EU e-government action plan 2016-2020: Accelerating the digital transformation of government. URL: https://digital-strategy.ec.europa.eu/en/library/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation-government (дата звернення: 08.11.2024).

355. European Commission. White Paper on Articial Intelligence - A European Approach to Excellence and Trust. Official website of the European Union. 2020. URL: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

356. Osavul. Advanced AI-Driven platform for information assessment and narrative impact assessment. URL: https://www.osavul.cloud/about-us (дата звернення: 01.06.2024).

357. Federal Emergency Management Agency (FEMA). URL: https://www.fema.gov/about (дата звернення: 05.10.2024).

358. Fire and Disaster Management Agency (FDMA) URL: https://www.fdma.go.jp/en/ (дата звернення: 05.10.2024).

359. GDPR: захист персональних даних по-європейськи і чому це важливо? Mikhailenko Platform. URL: https://www.mikhailenko.com.ua/09-05-2023/gdpr-zahyst-personalnyh-danyh-po-yevropejsky-i-chomu-cze-vazhlyvo-2/ (дата звернення: 15.02.2024).

360. Green Paper. Living and Working in the Information Society: People First. European Commission. Belgium, 1996. 33 p.

361. Law of civil defense. URL: https://www.nevo.co.il/law_html/Law01/125_001.htm (дата звернення: 15.09.2024).

362. Maria Andrea Latapie Aldana, Natalia Patricia Patino Espinosa. Digital Transformation, Retail and Regulatory Challenges in Mexico. CPI Antitrust Chronicle June 2022. URL: https://www.antitrustinstitute.org/wpcontent/uploads/2022/07/CPI_Market-Power-Supply-Chains_6.22.pdf

363. Mark Doctor, Chimai Ngo. Making our Roads Safer through a Safe System Approach. Public Roads – Winter 2022. Vol. 85 № 4. URL: https://highways.dot.gov/public-roads/winter-2022/01

364. Patwa T.Z., Moussa M. Transforming your culture of safety: Time to lead. Society of Petroleum Engineers – SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility 2018. Richardson: Society of Petroleum Engineers, 1-8. DOI: http://doi.org/10.2118/190671-ms

365. Robert T. Stafford Disaster Relief and Emergency Assistant Act, as amended by Public Law 106-390, October 30, 2000. URL: http://www.disastersrus.org/fema/stafact.htm (дата звернення: 05.10.2024).

366. Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017. URL: https://digitalstrategy.ec.europa.eu/en/news/ministerial-declarationegovernment-tallinn-declaration (дата звернення: 02.09.2024).

367. William A. Sodeman. Communications Decency Act, United States, 1996. URL: https://www.britannica.com/topic/Communications-Decency-Act (дата звернення: 02.06.2024).

368. What is GDPR, the EU’s new data protection law? GDPR.EU. URL: https://gdpr.eu/what-is-gdpr/ (дата звернення: 07.11.2024).

ДОДАТКИ

ДОДАТОК А

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Монографія:

1. Бондар Д.В. Адміністративно-правове регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності : монографія. Одеса: Видавництво «Юридика», 2025. 305 с.

Статті в періодичних фахових наукових виданнях України:

1. Бондар Д.В. Використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності: адміністративно-правові засади. *Право та державне управління*. 2024. № 3. С. 13–20. DOI: https://doi.org/10.32782/pdu.2024.3.2.

2. Бондар Д.В. Заходи забезпечення безпеки населення та територій у разі виникнення надзвичайних ситуацій: адміністративно-правова регламентація та напрями удосконалення в умовах цифровізації. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 4. С. 46–54. DOI: https://doi.org/10.32782/2408-9257-2024-4-8.

3. Бондар Д.В. Історіографія та методологія дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал*. 2024. № 11. С. 270–274. DOI: https://doi.org/10.32782/2524-0374/2024-11/61.

4. Бондар Д.В. Актуальні напрями удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Juris Europensis Scientia*. 2024. № 6.

С. 48–53. DOI: https://doi.org/10.32782/chern.v6.2024.9.

5. Бондар Д.В. Система принципів, напрямів та способів адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Київський часопис права*. 2024. № 4. С. 40–48. DOI: https://doi.org/10.32782/klj/2024.4.6.

6. Бондар Д.В. Адміністративно-правові засади використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності: сучасний стан та напрями удосконалення. *Право і суспільство*. 2024. № 6. С. 118–125. DOI: https://doi.org/10.32842/2078-3736/2024.6.18.

7. Бондар Д.В. Особливості понятійно-категоріального апарату та основні наукові підходи до дослідження адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний вісник*. 2024. № 6. С. 30–38. DOI: https://doi.org/10.32782/yuv.v6.2024.4.

8. Бондар Д.В. Досвід адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності в Європейському Союзі. *Правові новели*. 2024. № 24. С. 68–76. DOI: https://doi.org/10.32782/ln.2024.24.10.

9. Бондар Д.В. Особливості адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в США. *Держава та регіони. Серія: Право*. 2024. № 4. С. 51–58. DOI: https://doi.org/10.32782/1813-338X-2024.4.7.

10. Бондар Д.В. Адміністративно-правові засади забезпечення безпеки життєдіяльності та цивільного захисту в Японській Державі в умовах цифровізації. *Право та державне управління*. 2024. № 4. С. 36–45. DOI: https://doi.org/10.32782/pdu.2024.4.5.

11. Бондар Д.В. Особливості адміністративно-правового регулювання у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах воєнного стану. *Науковий вісник Міжнародного гуманітарного університету. Серія: «Юриспруденція».* 2024. № 72. С. 30–35. DOI: https://doi.org/10.32782/

2307-1745.2024.72.5.

12. Бондар Д.В. Безпека життєдіяльності в умовах інформаційного суспільства: актуальні питання та адміністративно-правові засоби їх вирішення. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 6. С. 90–97. DOI: https://doi.org/10.32782/2408-9257-2024-6-14.

13. Бондар Д.В. Забезпечення безпеки життєдіяльності та цивільний захист: співвідношення понять та особливості адміністративно-правового регулювання. *Науковий вісник публічного та приватного права*. 2024. № 6. С. 35–43. DOI: https://doi.org/10.32844/2618-1258.2024.6.6.

14. Бондар Д.В. Історія становлення та розвитку органів публічної адміністрації у сфері забезпечення безпеки життєдіяльності та цивільного захисту в контексті адміністративно-правового регулювання та цифровізації їх діяльності. *Правова позиція*. 2024. № 4(45). С. 82–89. DOI: https://doi.org/10.32782/2521-6473.2024-4.15.

15. Бондар Д.В. Реалізація публічних та приватних інтересів в процесі адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал*. 2024. № 10. С. 654–657. DOI: https://doi.org/10.32782/2524-0374/2024-10/156.

16. Бондар Д.В. Цифровізація систем цивільного захисту та забезпечення безпеки життєдіяльності: актуальні питання правового регулювання та матеріально-технічного забезпечення. *Юридичний науковий електронний журнал*. 2024. № 12. С. 543–546. DOI: https://doi.org/10.32782/2524-0374/2024-12/126.

17. Бондар Д.В. Адміністративно-правове регулювання захисту персональних даних та інформаційної безпеки у сфері забезпечення безпеки життєдіяльності. *Юридичний науковий електронний журнал*. 2025. № 1. С. 601–605. DOI: https://doi.org/10.32782/2524-0374/2025-1/140.

18. Бондар Д.В. Адміністративно-правове регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності. *Право і суспільство*. 2024. № 5. С. 665–672. DOI: https://doi.org/10.32842/2078-3736/2024.5.96.

Статті в періодичних наукових виданнях,
які індексуються в наукометричних базах Web of Sciences та Scopus:

1. Бондар Д., Бакала В. Протипожежний напрям діяльності національно-культурних товариств на Східній Галичині в 1920–1930-х рр. *Skhidnoievropeiskyi istorychnyi visnyk – East European Historical Bulletin*. 2024. № 33. С. 139–148. DOI: https://doi.org/10.24919/2519-058X.33.317455.

2. Bondar D. Legal means of ensuring life safety in the context of the digitalization of public administration and the economy. *Baltic Journal of Economic Studies*. 2024. Vol. 10. № 4. P. 101–105. DOI: https://doi.org/10.30525/2256-0742/2024-10-4-101-105.

3. Bondar D.V. The system of entities using information technologies in the field of life safety: administrative, legal and economic principles of effective functioning. *Baltic Journal of Economic Studies*. 2024. Vol. 10. № 5. P. 131–136. DOI: https://doi.org/10.30525/2256-0742/2024-10-5-131-136.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Бондар Д.В. Актуальні напрями адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Теоретичні та практичні проблеми реалізації норм права* : X Міжнародна науково-практична конференція, м. Кременчук, 5–7 грудня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 199–203. DOI: https://doi.org/10.36059/978-966-397-452-1-52.

2. Бондар Д.В. Принципи адміністративно-правового регулювання використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Proceedings of the international scientific conference*

“Theoretical foundations of law, public management and practice of their application”, Riga, the Republic of Latvia, December 25–26, 2024. Riga : Publishing House “Baltija Publishing”, 2024. P. 83–88. DOI: https://doi.org/10.30525/978-9934-26-526-6-18.

3. Бондар Д.В. Адміністративно-правове регулювання використання технології штучного інтелекту у сфері забезпечення безпеки життєдіяльності. *Становлення та розвиток правової держави: проблеми теорії та практики* : XVII Міжнародна науково-практична конференція, м. Миколаїв, 26 грудня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 93–95. DOI: https://doi.org/10.36059/978-966-397-463-7-23.

4. Бондар Д.В. Адміністративно-правова регламентація використання мобільного застосунку «Я – доброволець» з метою удосконалення систем забезпечення безпеки життєдіяльності та цивільного захисту в Україні. *Proceedings of the international scientific conference “The latest law developments”*, Wloclawek, Republic of Poland, April 3–4, 2024. Riga : Publishing House “Baltija Publishing”, 2024. P. 308–311. DOI: https://doi.org/10.30525/978-9934-26-432-0-72.

5. Бондар Д.В. Актуальні питання правового регулювання та матеріально-технічного забезпечення використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності. *Proceedings of the international scientific conference “Advances in law: the view of domestic and foreign scholars”*, Riga, the Republic of Latvia, October 3–4, 2024. Riga : Publishing House “Baltija Publishing”, 2024. P. 313–315. DOI: https://doi.org/10.30525/978-9934-26-493-1-80.

6. Бондар Д.В. Захист персональних даних у сфері забезпечення безпеки життєдіяльності: правове регулювання та європейські стандарти. *Proceedings of the international scientific conference “Scientific innovations in law amidst the impact of the Russian-Ukrainian war on the legal system”*, Riga, the Republic of Latvia, February 7–8, 2024. Riga : Publishing House “Baltija Publishing”, 2024. P. 316–319. DOI: https://doi.org/10.30525/978-9934-26-409-2-

76.

7. Бондар Д.В. Адаптація національного законодавства у сферах цивільного захисту, використання інформаційних технологій та забезпечення безпеки життєдіяльності до права Європейського Союзу. *Юридичні науки: проблеми та перспективи* : матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 23–24 лютого 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 293–297. DOI: https://doi.org/10.36059/978-966-397-374-6-84.

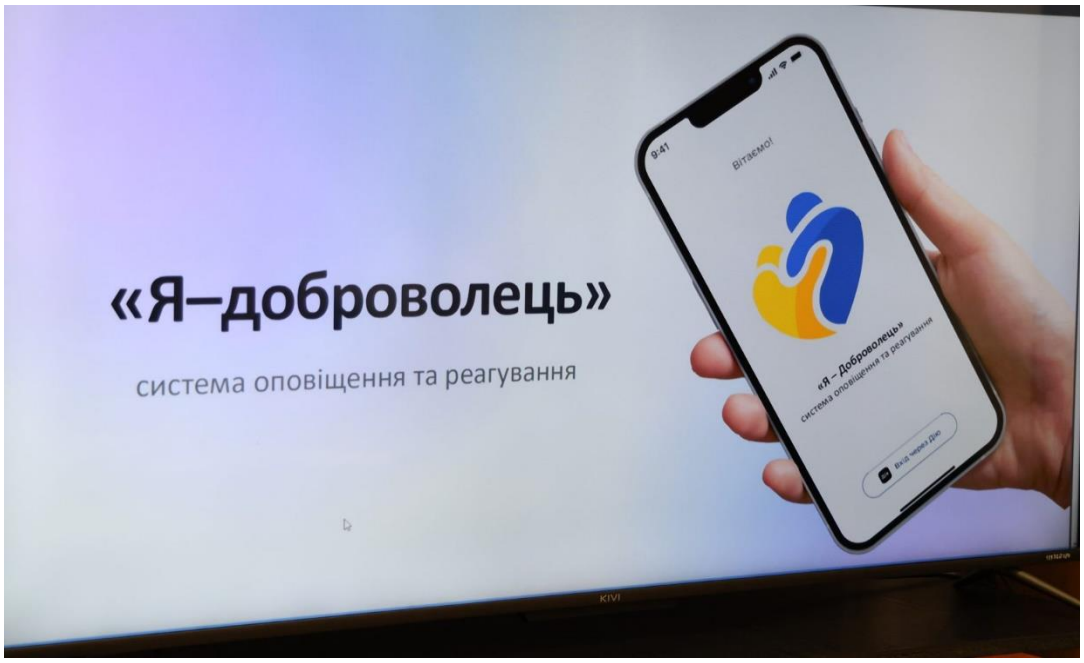
8. Бондар Д.В. Трансформація національного законодавства у сфері забезпечення безпеки життєдіяльності та цивільного захисту в умовах євроінтеграції та цифровізації. *Актуальні питання розвитку юридичної науки в період воєнного стану* : міжнародна науково-практична конференція, Науково-дослідний інститут публічного права, 17 травня 2024 р. Львів – Торунь : Liha-Pres, 2024. С. 363–367. DOI: https://doi.org/10.36059/978-966-397-395-1-107.

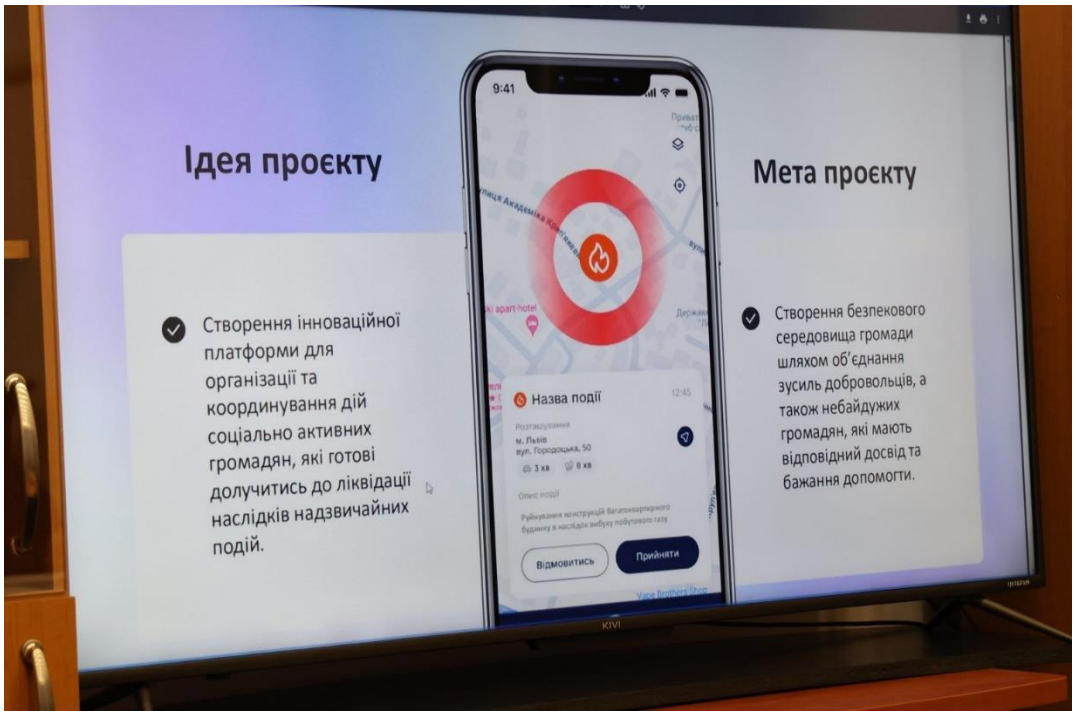
9. Бондар Д.В. Перспективні напрями удосконалення адміністративно-правового регулювання використання інформаційних технологій у сфері цивільного захисту та забезпечення безпеки життєдіяльності. *Теоретичні та практичні проблеми реалізації норм права* : матеріали IX Міжнародної науково-практичної конференції, м. Кременчук, 22–23 грудня 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 596–599. DOI: https://doi.org/10.36059/978-966-397-351-7-164.

10. Бондар Д.В. Адміністративно-правове регулювання використання інформаційних технологій у сфері цивільного захисту та забезпечення безпеки життєдіяльності в особливий період. *Восьмі Таврійські юридичні наукові читання* : матеріали міжнародної науково-практичної конференції, м. Київ, 16–17 червня 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 382–387. DOI: https://doi.org/10.36059/978-966-397-318-0-105.

ДОДАТОК Б

Система оповіщення та реагування «Я – доброволець»





A62C 99/00

СПОСІБ ЗАЛУЧЕННЯ ДОБРОВОЛЬЦІВ ДО ЛІКВІДАЦІЇ НАСЛІДКІВ НАДЗВИЧАЙНИХ ПОДІЙ ЗАСОБАМИ ІННОВАЦІЙНОЇ ІНФОРМАЦІЙНОЇ ПЛАТФОРМИ

Корисна модель відноситься до сфери забезпечення безпеки життєдіяльності людей в умовах надзвичайних ситуацій та надання допомоги у ліквідації їх наслідків шляхом організації та координування дій добровольців засобами інноваційної інформаційної платформи.

РЕФЕРАТ

Галузь застосування: корисна модель відноситься до сфери забезпечення безпеки життєдіяльності людей в умовах надзвичайних ситуацій та надання допомоги у ліквідації їх наслідків, шляхом організації та координування дій добровольців засобами інноваційної інформаційної платформи.

Суть винаходу: В основу корисної моделі поставлено завдання створення системи оповіщення та реагування на надзвичайні події на основі інформаційної системи, яка передбачає формування єдиної бази даних добровольців, їх залучення до ліквідації надзвичайних подій та координування дій шляхом використання мобільного додатка.

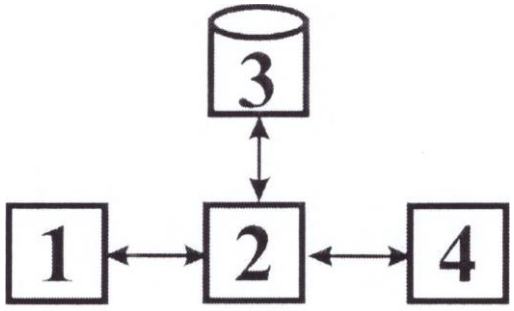
Технічний результат: Поставлене завдання вирішується створенням інформаційної системи, що включає адміністративну частину та базу даних добровольців і використовує мобільний додаток для оповіщення необхідної кількості користувачів із врахуванням їх геолокації, дати та часу залучення, можливості надання згоди щодо участі у ліквідації надзвичайної події, підрахунку кількості залучених добровольців, формування списків очікувань та корегування цієї кількості відповідно до оцінки обстановки на місці події.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб залучення добровольців до ліквідації наслідків надзвичайних подій засобами інноваційної платформи для автоматизації процесів оповіщення та координації дій добровольчого руху під час ліквідації наслідків масштабних надзвичайних подій, який **відрізняється тим,** що передбачає створення інформаційної системи з наявністю адміністративної частини та доступом до бази даних добровольців, а також забезпечуватиме можливість оповіщення необхідної кількості добровольців за допомогою мобільного застосунку із врахуванням зони їх геолокації, дати та часу залучення, а також збереженням можливості надання згоди щодо участі у ліквідації наслідків надзвичайної події та допомоги професійним рятувальним підрозділам.

КРЕСЛЕННЯ

СПОСІБ ЗАЛУЧЕННЯ ДОБРОВОЛЬЦІВ ДО ЛІКВІДАЦІЇ НАСЛІДКІВ НАДЗВИЧАЙНИХ ПОДІЙ ЗАСОБАМИ ІННОВАЦІЙНОЇ ІНФОРМАЦІЙНОЇ ПЛАТФОРМИ



Фіг.

1. Мобільний додаток
2. Адміністративна частина додатка
3. База даних добровольців
4. Керівник ліквідації надзвичайної ситуації