

БОНДАР Д. В.,

кандидат наук з державного управління,
ректор

(Львівський державний університет
безпеки життєдіяльності)

ORCID: 0009-0004-9571-7828

УДК 342.9 (477)

DOI <https://doi.org/10.32842/2078-3736/2024.5.96>

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ МОБІЛЬНИХ ЗАСТОСУНКІВ ТА ІНШОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ ТА БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Наукова публікація присвячена дослідженню актуальних питань адміністративно-правового регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності.

Зазначається, що 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 віднесено: мобільні застосунки, автоматизовані інформаційні системи, технологію штучного інтелекту. В якості позитивних прикладів використання мобільних застосунків у сферах цивільного захисту та забезпечення безпеки життєдіяльності наведено мобільний застосунок «Повітряна тривога» та чат-бот «Укриття».

З метою удосконалення національної системи цивільного захисту пропонується 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.

Формулюється висновок про необхідність оновлення програмного забезпечення, яке використовується в єдиній державній системі цивільного захисту шляхом адміністративно-правової регламентації та впровадження в практичну діяльність ДСНС України та інших суб'єктів владних повноважень (які реалізують державну політику у сфері цивільного захисту) технології штучного інтелекту.

Ключові слова: безпека життєдіяльності, цивільний захист, цифровізація, мобільні застосунки, програмне забезпечення, публічна адміністрація, інформаційні технології, автоматизовані системи, штучний інтелект, правове регулювання.

Bondar D. V. Administrative and legal regulation of the use of mobile applications and other software in the field of civil defense and life safety

The scientific publication is devoted to the study of current issues of administrative and legal regulation of the use of mobile applications and other software in the field of civil protection and life safety.

It is noted that modern information technologies allow to significantly improve the national civil protection system and mechanisms for ensuring life safety in general. Innovative information technologies used in the field of ensuring life safety



include: mobile applications, automated information systems, artificial intelligence technology. The mobile application «Air Alert» and the chat bot «Shelter» are given as positive examples of the use of mobile applications in the fields of civil protection and life safety.

In order to improve the national civil protection system, it is proposed to approve, by a joint order of the Ministry of Internal Affairs of Ukraine and the Ministry of Digital Transformation of Ukraine, 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.

A conclusion is formulated on the need to update the software used in the unified state civil protection system through legal regulation and the introduction of artificial intelligence technology into the practical activities of the State Emergency Service of Ukraine and other subjects of government authority (which implement state policy in the field of civil protection).

Key words: *life safety, civil protection, digitalization, mobile applications, software, public administration, information technologies, automated systems, artificial intelligence, legal regulation.*

Актуальність теми. 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.

Таким чином, актуальним є дослідження питання адміністративно-правового регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності.

Актуальні питання забезпечення безпеки життєдіяльності та цивільного захисту завжди знаходились в 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, Д. Біленька, О. Берназюк, М. Віхляєв, О. Гунбіна, К. Дубова, Т. Ковальова, Т. Коломоєць, О. Комаров, А. Комзюк, А. Краковська, І. Лопушинський, А. Омельченко, І. Тищенко 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, М. Бабик, Д. Біленької, О. Берназюка, Д. Бондара, О. Гунбіної, Т. Ковальової, О. Комарова, А. Краковської, Н. Литвин, І. Лопушинського, К. Оксютенка, А. Омельченка, Р. Стефанчука, І. Тищенкої.

Проте, питання адміністративно-правового регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності ще не були предметом окремого дослідження, що актуалізує необхідність підготовки даної публікації.

Постановка завдання. Метою публікації є дослідження актуальних питань адміністративно-правового регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності.

Методологія даної публікації традиційно об'єднує три групи методів наукового пошуку. Першу групу складають філософські методи дослідження, а саме, метод діалектики, його закони та прийоми (єдності та боротьби протилежностей, переходу кількісних змін у якісні, «заперечення заперечення»), а також метод метафізики. Серед загальнонаукових методів дослідження (друга група методів) більшою мірою застосовуються прийоми логіки (аналіз, синтез, дедукція, індукція, порівняння), системний та структурно-функціональний методи. Третю групу складають спеціально-юридичні методи дослідження, серед яких більшою мірою застосовуються формально-юридичний метод та метод юридичного моделювання.

Також, враховуючи тему дослідження, активно використовуються такі наукові підходи як: інструментальний, цивілізаційний, телеологічний та синергетичний.

Результати дослідження. 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).

На окрему увагу заслуговує використання інформаційних технологій у сфері забезпечення безпеки життєдіяльності, яка включає і єдину державну систему цивільного захисту.

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 [1], 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.

Вказаний застосунок інформує про початок і завершення повітряних, хімічних, техногенних та інших тривог системи цивільної оборони. Причому він надсилає сигнали навіть



у беззвучному або сплячому режимі смартфона. 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».

Так, у Львівському державному університеті безпеки життєдіяльності 28 лютого 2024 року відбулося виїзне засідання Комітету Верховної Ради України з питань екологічної політики та природокористування на тему: «Про стан функціонування добровільної та місцевої пожежної охорони» [2].

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» [2].

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 [2].

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.

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. 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. Водночас відсутність концептуальних засад державної політики в галузі штучного інтелекту не дозволяє створювати та розвивати конкурентоспроможне середовище в зазначених сферах діяльності [3].

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 [3].

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 [3].

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 [3].

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 [4], Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 р. № 685/2021 [5] та Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 [6].

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.

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) [7].

До засобів криптографічного захисту інформації належать апаратні, програмні та апаратно-програмні системи і комплекси, що реалізують криптографічні алгоритми перетворення інформації [7].

Правовою основою криптографічного захисту інформації є Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР [8]. 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) [9].

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» передбачено, 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 [4].

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 [10].

Отже, мобільні застосунки та інше програмне забезпечення, за умов належної адміністративно-правової регламентації, здатні суттєво удосконалити національну систему цивільного захисту та механізм забезпечення безпеки життєдіяльності в цілому.

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.

Висновки. Проведене дослідження актуальних питань адміністративно-правового регулювання використання мобільних застосунків та іншого програмного забезпечення у сфері цивільного захисту та безпеки життєдіяльності дозволило сформулювати наступні висновки:

- 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, технологія штучного інтелекту;

- 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;

- збереження важливої інформації у сфері цивільного захисту та забезпечення безпеки життєдіяльності доцільно здійснювати на декількох альтернативних серверах, причому таку інформацію варто зберігати не тільки на національних носіях, але й на серверах, які розташовані в зарубіжних країнах, що мають надійні партнерські відносини з Україною;



– 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;

– існує реальна потреба 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.

Перспективність подальшого дослідження даної тематики обумовлена необхідністю формулювання конкретних пропозицій щодо внесення змін до чинного адміністративного законодавства з урахуванням зарубіжного досвіду правового регулювання відповідної сфери суспільних відносин.

Список використаних джерел:

1. Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту: постанова Кабінету Міністрів України від 27 вересня 2017 р. № 733. Дата оновлення: 13.03.2024. URL: <https://zakon.rada.gov.ua/laws/show/733-2017-%D0%BF#Text> (дата звернення: 07.11.2024).
2. «Я – доброволець»: в Україні презентували концепцію інноваційної безпекової платформи. Міністерство внутрішніх справ України. Пресцентр. Новини. 28.02.2024. URL: <https://mvs.gov.ua/news/ia-dobrovolec-v-ukrayini-prezentovali-koncepciiu-innovaciinoyi-bezpekovoii-platformi> (дата звернення: 05.11.2024).
3. 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: 05.11.2024).
4. 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).
5. 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).
6. 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).
7. 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).
8. 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-vr?find=1&text=крипто#w1_1 (дата звернення: 02.11.2024).
9. 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).
10. Положення про Міністерство цифрової трансформації України, затверджене постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856. Дата оновлення: 13.01.2024. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-p/ed20240113#Text> (дата звернення: 02.11.2024).

