

Цифровізація мобілізаційного процесу: виклики та ризики

Шевчук Ю. А.¹

Опубліковано	Секція	УДК
28.04.2025	Право	341.636(045)
DOI: https://doi.org/10.5281/zenodo.15783301		

Анотація. Цифровізація є процесом широкого загальносуспільного запровадження цифрових технологій. Важливою сферою цифровізації є оборона та така її необхідна складова як належний мобілізаційний процес. Нині відбувається активне запровадження цифрових технологій у мобілізаційний процес. Попри скорочення часу обміну даними в мобілізаційному процесі та фактичного полегшення взаємодії учасників відносин у сфері мобілізації цифровізація тут має ряд труднощів та навіть небезпек. Проблемами цифровізації мобілізаційного процесу сьогодні є: недостатня інтеграція різних цифрових систем, що використовуються у мобілізаційному процесі; прогалини правового регулювання відносин у сфері цифровізації мобілізаційного процесу; відсутність стратегічного планування цифровізації мобілізаційного процесу; проблеми кадрового, технологічного та фінансового забезпечення цифровізації мобілізаційного процесу; ризик впливу технологічних негараздів на практичні аспекти цифровізації мобілізаційного процесу; відсутність загальнодоступності ресурсів цифровізації мобілізаційного процесу через майнове розшарування та технологічні проблеми, спричинені масованими обстрілами інфраструктурних об'єктів з боку агресора; кібернетично-безпекові загрози, що пов'язані із викраденням, знищенням чи спотворенням інформації, порушенням законодавства про захист персональних даних та захист інформації, проникненням до захищених ресурсів, що є носіями інформації у сфері національної безпеки та оборони тощо.

Зазначені загрози потребують реагування з боку фахового середовища та належної відповіді з боку законодавця, адже цифровізація мобілізаційних процесів стосується не лише питання надання послуг громадянам з боку держави, а в першу чергу впливає на питання забезпечення безпеки та оборони, що є надактуальним за умов збройної агресії проти України.

Ключові слова: інформатизація оборони, інформаційна безпека у сфері оборони, інформатизація за умов воєнного часу, кібербезпека у сфері оборони, інформатизація за умов особливого періоду.

Abstract. Digitalization is the process of widespread societal implementation of digital technologies. One of the most crucial areas of digitalization is defense and its indispensable component — an effective mobilization process. Today, digital technologies are being actively introduced into the mobilization process. Despite the reduction in data exchange time and the facilitation of interaction among participants in mobilization-related relations, digitalization in this field faces a number of challenges and even threats. The current problems of digitalizing

¹ аспірант кафедри адміністративного права та поліцейської діяльності Навчально-наукового інституту з підготовки фахівців для підрозділів кримінальної поліції, Львівський державний університет внутрішніх справ

the mobilization process include: insufficient integration of various digital systems used in mobilization; legal gaps in the regulation of digitalization-related relations; lack of strategic planning for digitalizing the mobilization process; issues related to staffing, technological capacity, and financial support; risks associated with technological failures affecting practical aspects of digitalization; the lack of public access to digitalization resources due to property stratification and infrastructure damage caused by massive enemy shelling; and cybersecurity threats related to data theft, destruction, distortion, violation of personal data protection laws, and unauthorized access to classified resources containing national security and defense information.

These challenges require a professional response and appropriate legislative action, as the digitalization of mobilization processes is not merely a matter of public service delivery but, above all, a critical component of national security and defense, especially under the conditions of armed aggression against Ukraine.

Keywords: defense informatization, information security in defense, wartime informatization, cybersecurity in the defense sector, informatization during special periods.

Вступ

Цифровізація є інструментом широкого соціального запровадження цифрових технологій. Сьогодні цифровізація є викликом, що вимагає докладання значних зусиль з боку держави, суспільства, організацій та окремих осіб. Війна, що її веде агресор проти України, здійснюється зі застосуванням з боку загарбника найсучасніших технологій, що вимагає належної відповіді. Таким чином, оборона спирається значною мірою на технологічні інновації, використання модерних цифрових технологій. Вагомим та необхідним елементом оборони є належний рівень мобілізаційного процесу, де впровадження цифровізації є необхідною вимогою сучасності. Проте, як необхідність цифровізації є викликом для сфери оборони, так само викликом значною мірою стає і вже запроваджена цифровізація в цій царині, зокрема у мобілізаційному процесі. Ризики пов'язані із кібербезпекою, доступністю та безперервністю цифрових технологій, оперативністю правого регулювання, єдністю цифровізації сфери оборони та суміжних соціальних галузей є вкрай гострими.

Загалом питання цифровізації мобілізаційного процесу, його викликів та ризиків є особливо актуальним та потребує окремого і нагального дослідження.

Окремі аспекти викликів та ризиків цифровізація мобілізаційного процесу розглядали зокрема такі науковці, як Гончарук Н. М., Дзюбук Т.М., Кравець О.М., Шевчук О. В. та інші вчені. Водночас у цілому питання викликів та ризиків цифровізації мобілізаційного процесу потребує окремого дослідження.

Метою дослідження є вивчення питання викликів і ризиків цифровізації мобілізаційного процесу в контексту. Задля досягнення мети дослідження передбачається виконання наступних завдань: з'ясування сутності цифровізації, її завдань в контексті оборони та мобілізаційного процесу; виявлення переваг та недоліків запровадження цифровізації мобілізаційного процесу; розкриття викликів та ризиків цифровізації мобілізаційного процесу.

Результати

Основним нормативно-правовим актом, що встановлює правові основи мобілізації в Україні є Закон України «Про мобілізаційну підготовку та мобілізацію» від 21.10.1993 № 3543-XII (далі – ЗУ «Про мобілізацію»), згідно із змістом положень абз. 4 ч. 1 ст. 1 якого під мобілізацією слід розуміти комплекс заходів, що здійснюються задля планомірного переведення національної економіки, діяльності державних органів, органів місцевого самоврядування, підприємств, установ та організацій на

функціонування за умов особливого періоду, а Збройних Сил України, інших військових формувань, сил цивільного захисту - на організацію та штати воєнного часу [1].

У згоді з положеннями ч. 1 ст. 3 ЗУ «Про мобілізацію», мобілізація виступає складником сукупності заходів, що їх здійснюють задля забезпечення оборони держави, окрім цільової мобілізації. Таким чином, належне здійснення мобілізації є складовою захисту всієї держави, а отже і її громадян та її населення в широкому розумінні. Інакше кажучи, дієвість мобілізації впливає на спроможність держави захистити та гарантувати права людини в разі наявності відповідних загроз.

Одним із важливих напрямків соціальних перетворень сьогодення є цифровізація, що не оминає і сфери оборони.

У згоді зі положеннями п. 25 ч. 1 ст. 1 Закону України «Про Національну програму інформатизації» від 01.12.2022 № 2807-IX (далі – ЗУ «Про програму», цифровізація є процесом впровадження цифрових технологій до кожної царини суспільного життя [2]. Таке визначення вказує на масштабність завдання цифровізації, але воно ж з цієї причини пропонує і доволі широке розуміння цього явища. Водночас у згоді зі змістом положень Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки, схваленої розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р (далі – Концепція), цифровізація є насиченням фізичного світу електронно-цифровими пристроями, засобами, системами й налагодженням електронно-комунікаційного обміну між ними, що фактично робить можливою інтегральну взаємодію віртуального й фізичного, тобто створює кіберфізичний простір [3]. Таке визначення дає вже чіткіші ознаки цифровізації, як соціально-технологічного явища.

Також відповідно до змісту положень Концепції, основною метою цифровізації є досягнення цифрової трансформації існуючих й створенні нових галузей економіки, а так само перетворень царин життєдіяльності на нові більш дієві й модерні. При цьому зазначено, що такого роду зростання має можливість виключно тоді, коли ідеї, дії, ініціативи й програми, що стосуються цифровізації, будуть інтегрованими у тому числі до національних, регіональних, галузевих стратегій та програми розвитку.

Також у Концепції вказано, що цифровізація виступає визнаним механізмом економічного зростання через здатність технологій чинити позитивний вплив на дієвість, результативність, вартість і якість економічної, громадської й особистої діяльності.

Концепція затверджує ряд принципів цифровізації, дотримання яких є визначальним для створення, реалізації й користування перевагами, що їх надають цифрові технології.

Принцип 1 вимагає, щоби цифровізація забезпечувала кожному громадянину рівний доступ до послуг, інформації та знань, що надаються на основі інформаційно-комунікаційних та цифрових технологій. Зазначається, що формування цифрових інфраструктур є основним чинником розширення доступу громадян до глобального інформаційного середовища й знань. Окремо підкреслюється, що 2011 року вільний доступ до мережі Інтернет визнано з боку ООН в якості фундаментального права людини - цифрового права. Тут варто зазначити, що питання цифровізації окремих складових мобілізаційного процесу безперечно є нагальною потребою як чинника гарантування цифрового права громадян. Проте мова може йти про цифровізацію саме окремих напрямків мобілізаційної діяльності, а саме тих її напрямків, де це буде виправдано питаннями оборони держави та безпеки її громадян та усіх учасників мобілізаційного процесу.

Згідно із принципом 2 цифровізація має бути спрямованою на формування переваг в багатоманітних сферах щоденного життя. В Концепції зазначено щодо цього принципу, що він зокрема полягає у підвищенні якості надання послуг з гарантування громадської безпеки тощо. Оскільки вказаний перелік не є обмеженим, то варто припустити, що

окремі напрямки національної та оборони можуть так само мати результатом цифровізації покращення якості надання послуг. Стосовно процесу мобілізації, то цифровізація в такій сфері має покращити якість послуг, що надаються громадянам-учасникам мобілізаційних відносин.

Принцип 3 передбачає, що цифровізація реалізується механізмом економічного зростання через підвищення дієвості, продуктивності й конкурентоспроможності від використання цифрових технологій. Зазначено, що таким принципом передбачено досягнення цифрової трансформації галузей економіки, сфер діяльності, набуття ними нових конкурентних якостей і властивостей. При цьому всеохопність цифровізації має ціллю комплексну й глибоку трансформацію наявних аналогових економічних, соціальних систем й сфер в нову цінність і якість з метою їх дієвості, розвитку, зручності використання тощо. Водночас цифровізація формує нові можливості для інвестиційної діяльності, нові робочі місця, надає імпульс розвитку національної ІТ-індустрії.

Згадані у принципі 3 Концепції положення значною мірою підлягають застосуванню у процесі мобілізації, оскільки нові технології не лише полегшують комунікацію між усіма учасниками мобілізації, але вимагають залучення фахівців та їх розроблення, запровадження, підтримання, просування та подальшої модернізації. Мова йде як про розроблення мобільних застосунків мобілізаційного напрямку для широкого їх використання громадянами України, так і про впровадження електронних ресурсів для суб'єктів владних повноважень у сфері мобілізаційних відносин. Окремим напрямком стає питання інформування громадськості про порядок та цілі мобілізаційного процесу, де цифрові технології є важливим джерелом донесення знань у цій галузі.

Принцип 4 передбачає, що цифровізація має сприяти розвитку інформаційного соціуму та ЗМІ. В такому разі сформоване інформаційне суспільство саме по собі виступатиме важливим чинником належного рівня правової культури з питань мобілізації, що має сприяти належному рівні мобілізаційного процесу.

Зі змісту принцип 5 випливає, що цифровізація має орієнтуватися на міжнародну, європейську й регіональну співпрацю зокрема з ціллю інтеграції України до Європейського Союзу. При цьому зазначено, що інтегрування України до європейських та глобальних систем й інфраструктур є в тому числі результатом свідомого й справдішнього упровадження інформаційно-комунікаційних й цифрових технологій. Варто зазначити, що використання досвіду ЄС у царині правового регулювання відносин мобілізації, зокрема в частині їх цифровізації, є не лише інструментом поліпшення процесу мобілізації, а й кроком на шляху до отримання Україною статусу повноправного члена Європейського Союзу. Водночас запровадження будь-яких позанаціональних стандартів у мобілізаційний процес в Україні має відбуватись виключно із врахуванням вимог національної безпеки, оборони та прав і свобод громадян України та людини в цілому.

В згоді із принципом 6 основою цифровізації є стандартизація, як один з головних чинників успішності її реалізації. Зазначено, що формування тільки на українських стандартах цифрових систем, платформ й інфраструктур, що повинні бути використані громадянами, підприємцями й державою для участі, конкуренції й успіху с глобальною економікою й на відкритих ринках, є неприпустимим. Водночас вказано, що винятком можуть бути відповідні програми в царині оборони й безпеки, де застосування інших стандартів (національних, міждержавних) є аргументованим. Варто зазначити, що до такого виняткового напрямку цифровізації на основі національних стандартів має належати й цифровізація процесів мобілізації, оскільки йдеться не про входження у глобальні відносини, а про національну безпеку та захист прав і свобод громадян України та людини загалом.

Принцип 7 передбачає, що цифровізація має супроводжуватись підвищенням рівня довіри й безпеки. Така вимога безпосередньо стосується мобілізаційного процесу та сфери оборони в цілому. При цьому в Концепції зазначено, що інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя й прав користувачів цифрових технологій, зміцнення й захист довіри в кіберпросторі є у тому числі передумовами одночасного цифрового розвитку й відповідного попередження, усунення та управління супутніми ризиками. Слід зазначити, що саме це питання й викликає найбільше заперечень широкому процесу цифровізації мобілізаційного процесу, оскільки йдеться про необхідність захисту величезного обсягу інформації, що його захищеність є вкрай важливою передумовою забезпечення національної безпеки та гарантування найважливіших прав і свобод людини і громадянина.

Принцип 8 полягає у тому, що цифровізація має перебувати в якості об'єкта фокусного і комплексного державного управління. Зазначено, що на шляху до цифровізації країни основними завданнями держави є корекція недоліків ринкових механізмів, здолання інституційних і законодавчих перепон, започаткування проєктів цифрових трансформацій національного рівня й залучення відповідних інвестицій, стимулювання розвитку цифрових інфраструктур, формування потреб у використанні цифрових технологій громадянами й розвитку відповідних цифрових компетенцій, створення відповідних стимулів й мотивацій з метою підтримки цифрового підприємництва та цифрової економіки. Таке зауваження є особливо важливим щодо заходів із цифровізації мобілізаційного процесу, де державні інституції мають одночасну здійснювати просвітницьку діяльність, популяризувати саму ідею цифровізації заходів у сфері мобілізації, забезпечувати взаємодію між усіма державними інституціями, муніципальними учасниками вказаної царини, господарюючими суб'єктами відносин у сфері мобілізації та громадянами, здійснювати неухильний контроль за дотриманням кібербезпеки та національної безпеки в цій сфері та оперативно реагувати на динаміку ситуації у сфері національної безпеки та оборони, вносячи відповідні зміни у цифровізаційну складову процесу мобілізації. Цифровізація мобілізаційного процесу має здійснюватись виключно державою із мінімізацією залучення позадержавного сектору, оскільки йдеться не лише про надання відповідних послуг громадянам, але й про питання їх безпеки та безпеки держави й суспільства в цілому.

Слід зазначити, що питання цифровізації безпосередньо пов'язується із сферою оборони й на рівні положень Закону України «Про програму», в ч. 1 ст. 8 якого зазначено, що національна програма інформатизації формується виходячи із довгострокових пріоритетів соціально-економічного, науково-технічного, національно-культурного розвитку держави зі врахуванням світових напрямів розвитку й досягнень в сфері інформатизації та є спрямованою на розв'язання проблем розвитку інформаційного суспільства, підвищення дієвості й результативності державного управління, національної безпеки та оборони, демократизації суспільства. При цьому в згоді зі положеннями п. 14 ч. 1 ст. 1 ЗУ «Про програму», інформатизація - це єдність взаємопов'язаних організаційних, правових, політичних, суспільно-економічних, науково-технічних, технологічних й виробничих процесів, що є спрямованими на формування умов гарантування розросту інформаційного суспільства та впровадження інформаційно-комунікаційних та цифрових технологій. Водночас як зазначено вище в згоді з п. 25 ч. 1 ст. 1 ЗУ «Про програму», цифровізація є процесом запровадження цифрових технологій в усі царини суспільного життя.

Отже, цифровізація є складовою інформатизації. Тобто, законодавець прямо пов'язує здійснення інформатизації, частиною якої і є цифровізація, із підвищенням дієвості й результативності національної безпеки та оборони. В такому разі цифровізація із погляду положень ЗУ «Про програму» не може оминати мобілізаційного процесу.

Де-факто заходи із цифровізації мобілізаційного процесу практично одразу дали відчутний ефект. Як зазначає Шевчук О.В., впровадження цифрових платформ, як-от система резервістів «Резерв+», значною мірою скоротило час на підготовку й координацію між державними органами [4, с. 94].

Дзюбук Т.М. звертає увагу на те, що попри запроваджені перетворення, мобілізаційний процес має справу із низкою викликів [5, с. 88]. Однією із основних проблем лишається недостатність інтегрування цифрових систем зі міжвідомчими платформами, що робить складнішою координацію між державними органами й військовими структурами, на чому акцентує Кравець О.М. [6, с. 27]. Дослідник вивчає питання запровадження електронного реєстру військовозобов'язаних й електронного кабінету резервіста й наголошує на тому, що такі цифрові можливості суттєво скорочують час мобілізації й оптимізують адміністративні процеси, проте науковець відзначає наявність потреби у розробці чітких правових механізмів стосовно захисту персональних даних у згоді з вимогами національного законодавства й міжнародних стандартів, зокрема Загального регламенту про захист даних (GDPR) [6, с. 26].

Ба більше, Гончарук Н.М. зауважує, що правові прогалини в регулюванні контрактних зобов'язань резервістів, а також механізми захисту персональних даних за умов цифровізації потребують наступного вдосконалення [7, с. 103].

Як зауважує Дзюбук Т.М., електронний кабінет призовника та резервіста, що його запроваджено Законом України від 16 січня 2024 року № 3125-ІХ «Про внесення змін до деяких законодавчих актів України щодо удосконалення окремих питань мобілізаційної підготовки та мобілізації», є одним із ключових інструментів цифровізації [5, с. 89-90]. Така система дає змогу військовозобов'язаним отримувати актуальну інформацію про мобілізаційний статус, подавати заяви на відстрочку, оновлювати дані про місце проживання й здійснювати інші адміністративні дії без потреби у фізичному відвідуванні територіальних центрів комплектування [4, с. 90]. Дзюбук Т.М. вважає, що запровадження такого інструменту дає змогу мінімізувати бюрократичні ризики, підвищити прозорість мобілізаційних процедур та забезпечити належний захист персональних даних у згоді з європейськими стандартами кібербезпеки [5, с. 90]. Дослідник також зазначає, що українська система мобілізації в активний спосіб адаптується до нормативних стандартів НАТО, що включає класифікацію військового резерву, цифровізацію мобілізаційних процедур та оновлення стандартів ротації. Інтеграція таких норм сприяє підвищенню рівня підготовки резервістів, уніфікації мобілізаційного процесу та забезпечити його відповідності міжнародним практикам [5, с. 90].

Цифровізація мобілізаційного процесу в цілому має ряд викликів, що потребують реагування та подолання. До таких проблемних питань варто віднести брак чіткої стратегії впровадження такої цифровізації, що вимагає поступове нарощування фінансування, поліпшення технічного забезпечення військових та цивільних владних інституцій, безперервне навчання персоналу, подолання кадрового дефіциту, недостатність правового регулювання процесів цифровізації у сфері мобілізації та складність питання про застосування юридичної відповідальності за порушення вимог законодавства, що передбачає цифровізацію у сфері мобілізації. Стосовно прогалин правового регулювання цифровізації мобілізаційного процесу, то варто зазначити, що цьому питанню практично не надано уваги з боку законодавця ані в ЗУ «Про мобілізацію», ані в ЗУ «Про програму», ані в Концепції.

Шевчук О.В. зазначає, що загрозою є питання інтеграції електронних мобілізаційних платформ із державними інформаційними системами [4, с. 90]. Впровадження Єдиного державного реєстру військовозобов'язаних та цифрових платформ, як-от «Резерв+», безпосередньо сприяло автоматизації мобілізаційних процесів, але недостатність координування дій між державними органами й відсутність

уніфікованої системи даних обмежують дієвість їхнього використання [4, с. 92]. Це формує правові й технічні перешкоди для обміну інформацією між військовими адміністраціями, Міністерством оборони України, Міністерством цифрової трансформації України та іншими державними органами [4, с. 94].

Слід додати, що цифровізація мобілізаційного процесу також має своїм недоліком постійність кіберзагроз, що знаходить своє вираження у формах несанкціонованого доступу до інформації, цифрових атак, витоку даних тощо. Проблемою є й також питання цифрової нерівності, оскільки нерідко спостерігається нерівний доступ до технологій та цифрових навичок, що може мати місце серед усіх учасників відносин у сфері мобілізації. Проблемою може бути й скорочення працівників та виникнення безробіття через автоматизацію елементів мобілізаційного процесу. Загрози зберігаються й у сфері інформаційної безпеки, що може знаходити своє вираження у завданні шкоди мобілізаційному процесу через поширення із використанням інструментів цифровізації недостовірної інформації та дезінформації.

На сьогодні питання цифровізації мобілізаційного процесу перебуває у колі пріоритетів для законодавця.

Нещодавно парламент України прийняв у цілому як закон законопроект № 12066 “Про внесення змін до деяких законів України щодо створення і функціонування Єдиного державного реєстру військовослужбовців та удосконалення порядку ведення військового обліку” (далі – Проект) [8]. Цей документ розроблено із ціллю формування єдиної бази даних про військовослужбовців Збройних Сил України й Державної спеціальної служби транспорту, тобто - Реєстру військовослужбовців.

Відповідний проект закону вже було прийнято за основу 18 грудня 2024 року, проте на нього наклав вето глава держави у зв'язку із внесенням до Реєстру даних про військовослужбовців розвідки й СБУ.

Тепер прийнятий 17 червня 2025 року законопроект передбачає автоматичне присвоєння кожному військовослужбовцю ID ідентифікатора для однозначної ідентифікації військовослужбовця та використання в інформаційно-комунікаційних системах, зокрема на Державному вебпорталі електронних публічних послуг у сфері національної безпеки й оборони, а також для надання публічних (електронних публічних) послуг військовослужбовцям та членам їх сімей, що їх особливості надання у сфері національної безпеки й оборони визначено окремим законом.

Також остаточна редакція прийнятого законопроекту передбачає, що до Реєстру включається наступна інформація про військовослужбовця: ПІБ військовослужбовця; його стать; дата народження; реєстраційний номер облікової картки платника податків або паспортні дані (за відповідних підстав); відомості про видані військово облікові документи (номер документа, серія і дата видачі).

Водночас інша інформація про військовослужбовців, у тому числі відцифрований образ обличчя, може отримуватись Реєстром через електронну інформаційну взаємодію із інформаційно-комунікаційними системами і реєстрами, що їх передбачено цим Проектом, за дотримання вимоги про те, що таку інформацію не зберігатимуть та вона не накопичуватиметься у Реєстрі.

У Проекті так само зазначено, що інформація, що її внесено до Реєстру військовослужбовців, належить до інформації зі обмеженим доступом й вона не підлягає оприлюдненню.

При цьому в Проекті зазначено, що в разі звільнення із військової служби військовослужбовця ЗСУ або Державної спеціальної служби транспорту, інформація про такого військовослужбовця зберігається у Реєстрі до досягнення ним граничного віку перебування на військовій службі.

У випадку загибелі (смерті) військовослужбовця ЗСУ або Державної спеціальної служби транспорту, відомості про такого військовослужбовця зберігається у Реєстрі протягом 25 років від дня настання події.

Вилучення інформації з Реєстру у випадку переведення військовослужбовця ЗСУ чи Державної спеціальної служби транспорту до Служби безпеки України, розвідувальних органів України, інших військових формувань здійснюється на підставі відповідного звернення такого органу.

Також в Проекті зазначено, що Інформація з Реєстру військовослужбовців не підлягає оприлюдненню. Передача реєстрової інформації здійснюється у згоді із ч. 10 ст. 25-1 Закону України «Про військовий обов'язок і військову службу» від 25.03.1992 № 2232-ХІІ.

Як зазначають Луценко В.Р. та Пікуля Т.О., важливою вимогою, що висувається до процесу цифрових трансформацій, є вимога інформаційної безпеки. При цьому в Україні усі можливі ризики та небезпеки враховувати особливо важливо, оскільки, окрім вже відомих та «традиційних» викликів, наш інформаційний простір «обтяжений» війною, яка ведеться проти України [9, с. 63]. Безперечно, що таке зауваження стосується й цифровізації мобілізаційного процесу.

Загалом, як зазначає Маркевич К., загрози поширення цифрових технологій стосуються можливого зламу цифрових систем із несанкціонованим доступом до персональних даних. Йдеться про ризик втрати конфіденційності. Також технічні негаразди у роботі пристроїв можуть спричинити збій у програмному забезпеченні, що може призвести до отримання недостовірної або неактуальної інформації. Окремою проблемою є ризик цифрової поляризації простору. Існує велика частка населення, що перебуває за межею бідності. Тоді концентрація населення у мегаполісах, що є споживачами цифрових технологій, може створити загрозу територіальної цифрової нерівності та стратифікації соціуму. Варто зазначити, що питання поширеності бідності для України є однією із важливих проблем, що лише загострилась із початком повномасштабного вторгнення 2022 року. На сьогодні не усі учасники відносин у сфері мобілізації в Україні мають доступ до цифрових технологій та через низькі доходи просто не володіють пристроями, на які можна встановити відповідні мобільні додатки. Водночас має місце ризик, що перевагами цифрових технологій скористаються не усі верстви населення через відсутність доступу до сучасних цифрових з'єднань та цифрового обладнання, що може стати загрозою для соціальної згуртованості та інклюзивності та мати наслідком появу соціальних класів цифрової еліти і цифрових «ізгоїв» [10]. Стосовно останнього прогнозу Маркевич К. варто зазначити, що постійне технологічне оновлення засобів зв'язку, як головних інструментів застосування цифровізації у сфері мобілізації тягне за собою необхідність фінансових витрат, що не завжди доступні кожному учаснику відносин у сфері мобілізації. До прикладу, чергове оновлення мобільного за стосунку може перевершити технічні можливості засобу зв'язку особи, яка підлягає мобілізації, а придбання сучаснішого пристрою вимагає додаткових капіталовкладень, що не завжди є можливим.

Ще однією проблемою може стати ускладнення обміну інформацією у процесі практичного застосування цифровізації в сфері мобілізації, що має своєю причиною збройні атаки з боку агресора на технологічні об'єкти та інфраструктуру, що забезпечують сталість та безперервність обміну даними.

Висновки

Отже, цифровізація мобілізаційного процесу має ряд викликів та ризиків.

Попри скорочення часу обміну даними в мобілізаційному процесі та фактичного полегшення взаємодії учасників відносин у сфері мобілізації цифровізація тут має ряд труднощів та навіть небезпек. Проблемамаи є: недостатня інтеграція різних цифрових

систем, що використовуються у мобілізаційному процесі; прогалини правового регулювання відносин у сфері цифровізації мобілізаційного процесу; відсутність стратегічного планування цифровізації мобілізаційного процесу; проблеми кадрового, технологічного та фінансового забезпечення цифровізації мобілізаційного процесу; ризик впливу технологічних негараздів на практичні аспекти цифровізації мобілізаційного процесу; відсутність загальнодоступності ресурсів цифровізації мобілізаційного процесу через майнове розшарування та технологічні проблеми, спричинені масованими обстрілами інфраструктурних об'єктів з боку агресора; кібернетично-безпекові загрози, що пов'язані із викраденням, знищенням чи спотворенням інформації, порушенням законодавства про захист персональних даних та захист інформації, проникненням до захищених ресурсів, що є носіями інформації у сфері національної безпеки та оборони тощо.

Вказані виклики та загрози потребують ґрунтовного дослідження з боку практиків та науковців у сфері інформаційної безпеки, національної безпеки та оборони, мобілізаційного процесу та негайного реагування з боку законодавця.

Список використаних джерел:

1. Про мобілізаційну підготовку та мобілізацію: Закон України від 21.10.1993 № 3543-XII. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3543-12#Text> (дата звернення: 20.06.2025).
2. Про Національну програму інформатизації: Закон України від 01.12.2022 № 2807-IX. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text> (дата звернення: 20.06.2025).
3. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 № 67-р. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text> (дата звернення: 20.06.2025).
4. Шевчук О. В. Використання електронних платформ у військовому обліку: досвід України та країн НАТО. Наукові записки Національного університету оборони України. 2024. № 18, С. 89–95.
5. Дзюбук Т.М. Сучасні виклики правового регулювання мобілізації на військову службу в Україні. Європейський правничий часопис. 2025. Вип. 6, 7, С. 87-93. URL: <https://irback.e-u.edu.ua/server/api/core/bitstreams/6fbdfcb5-f317-4ccc-8f60-342b567022ed/content> (дата звернення: 20.06.2025).
6. Кравець О.М. Роль цифровізації в удосконаленні мобілізаційного процесу. Цифрові інновації в публічному управлінні. 2024. Т. 8. № 1, С. 24–31.
7. Гончарук Н. М. Проблеми адаптації мобілізаційних систем до умов воєнного стану. Кримінологічний журнал України. 2024. № 11, С. 101–108.
8. Законопроект № 12066 «Про внесення змін до деяких законів України щодо створення і функціонування Єдиного державного реєстру військовослужбовців та удосконалення порядку ведення військового обліку». База даних «Законопроекти». URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/44930> (дата звернення: 20.06.2025).
9. Луценко В.Р., Пікуля Т.О. Правове забезпечення цифрової трансформації в Україні. Науковий вісник Ужгородського Національного Університету. 2024. Серія ПРАВО. Випуск 81: частина 1, С. 61-67. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/03/11.pdf> (дата звернення: 20.06.2025).
10. Маркевич К. Не позитивами єдиними. Які небезпеки криються за цифровізацією. Інтернет-ресурс «Разумков». URL: <https://razumkov.org.ua/statti/ne-pozytyvamy-iedynymy-yaki-nebezpeky-kryiutsia-za-tsyfrovizatsiieiu> (дата звернення: 20.06.2025).

