УДК 364:004.056.5 **doi: 10.20998/2227-6890.2025.1.07**

Л.М. ГРЕНЬ, О.В. ГРИБКО

ГАРАНТУВАННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ СОЦІАЛЬНОЇ СФЕРИ

Розвиток інформаційно-комунікаційних технологій набуває все більших обертів у нашому сьогоденні, їх впровадження в усі сфери життя та цифровізація суспільного життя є невідворотним процесом, який притаманний роботі значній кількості сфер життя, в тому числі й соціальній. Разом з тим виникає питання захисту інформації та даних отримувачів публічних послуг – як соціальних, так і адміністративних послуг соціального характеру, – а поряд постає необхідність дотримання принципу прозорості роботи органів соціальної сфери, що ускладнює завдання гарантування кібербезпеки через неможливість "закриття" всієї інформації, яка надходить до соціальної сфери. У статті зроблено спробу розглянути вказане протиріччя.

Ключові слова: соціальна сфера, соціальний захист, цифровізація, інформаційно-комунікаційні технології, кібербезпека, соціальні послуги, адміністративні послуги соціального характеру.

L.M. HREN, O.V. GRYBKO

GUARANTEEING CYBERSECURITY IN THE CONDITIONS OF SOCIAL SPHERE'S DIGITIZATION

The development of information and communication technologies is gaining momentum in our current life, their implementation in all life spheres and the digitalization of public life is an inevitable process that is inherent in the work of a significant number of life spheres, including the social one. At the same time, the issue of protecting information and data of recipients of public services – both social and administrative services of a social nature – arises, and at the same time there is a need to adhere to the principle of transparency of the social sphere bodies' work, which complicates the task of guaranteeing cybersecurity due to the impossibility of "closing" all information that enters the social sphere. The article attempts to consider this contradiction.

Key words: social sphere, social protection, digitalization, information and communication technologies, cybersecurity, social services, administrative services of a social nature.

Постановка проблеми. Традиційно технології розвиваються швидше, ніж здатність людей передбачати їхній вплив на політичні, соціальні чи економічні системи. Тому влада багатьох країн та міжнародні організації намагаються впроваджувати закони, нормативні акти та системи управління, спрямовані на нормалізацію цього впливу. Однак результати цих зусиль часто менш передові, ніж технічний прогрес. Це особливо актуально для країн, де розширення комунікацій зростає набагато швидше, ніж здатність органів публічного управління, ринкової економіки та громадянського суспільства розвивати свої технічні та політичні можливості, щоб скористатися перевагами технологічного прогресу та водночас зменшити загрози, пов'язані з кіберінфраструктурою.

Стає необхідним гарантувати захист громадян та створювати правові інструменти, що забезпечують гарантії безпеки доступу до інформації, при цьому протидіючи кіберзагрозам у сфері її неправомірного використання. Розвиток цифрових технологій передбачає нові механізми управління, на які впливає політика, а взаємозв'язки між дедалі складнішими соціальними та технічними системами неминуче зростатимуть. На переконання П. Тіммерса, "кібербезпека стане дедалі важливішою темою для країн усього світу, створюючи процеси цифрової трансформації, які впливають на суспільства, економіки та політичні утворення" [30].

Ще одним важливим питанням у цьому контексті є аналіз взаємодії між технічною, соціальною та політичною сферами на локальному, національному та міжнародному рівнях. Відповідь на це питання є ключовим фактором для розуміння того, як кіберполітика та кібербезпека на вказаних рівнях можуть сприяти або перешкоджати інтересам суб'єктів соціальної взаємодії, що неможливо дослідити виключно формально. Крім того, у подальшому дослідження гарантування кібербезпеки може оцінити значна кількість людей, які володіють важливими даними про кібероперації, що не є відомими широкому загалу.

Відмітимо, що існує низка важливих політичних та соціальних питань, пов'язаних із захистом конфіденційності даних та наглядом за правоохоронними органами, які використовують кібертехнології для моніторингу суспільства. Таким чином, органам публічного управління та громадянському суспільству доведеться дійти згоди щодо кількості нових даних, яка має бути доступною для громадськості та які наслідки для захисту даних та конфіденційності можуть бути гарантовані.

Аналіз останніх досліджень і публікацій. Питанням кібербезпеки у різноманітних її аспектах присвячено значну кількість наукових праць: Т. Бернс, О. Васильківський, В. Горбулін, Н. Грицяк, М. Ковтун, Є. Котух, А. Монарха-Матлак, Г. Ніссенбаум, А. Семенченко Н. Ющенко

присвятили свої роботи розвитку електронного урядування та питанням кібербезпеки. Взаємозв'язок політик кібербезпеки та транспарентності розглянуто у роботах Р. Вебера, П. Гаврисяка, Дж. Кохена, Т. Ріда, П. Світая, Д. Скочиляс, П. Тіммерса.

Однак, незважаючи на велику кількість наукових робіт, тема специфіки використання цифрових інструментів для соціальної сфери залишається маловивченою. Необхідно зважити ризики від відкритості інформації та потенційні кіберзагрози, тому проблема розробки заходів з гарантування кібербезпеки у соціальній сфері на сучасному етапі стала актуальною як у практичному, так і в теоретичному плані.

Мета статті полягає у вивченні динаміки цифровізації соціальної сфери та підходів до політики кібербезпеки з урахуванням необхідності забезпечення як захисту персональних даних отримувачів соціальних послуг й адміністративних послуг соціального характеру, так і прозорості та підзвітності роботи органів соціальної сфери.

Виклад основного матеріалу. Цифровізація суспільного життя привела до його суттєвих змін, які насамперед дотичні до діяльності органів публічної влади, зокрема й органів соціальної сфери. Окрім того, що з'явилися нові моделі взаємодії цих структур із громадянським суспільством, вплив цифровізації роботи органів соціальної сфери спричинив перетворення в інших аспектах їх діяльності [2; 8]. Розглянемо їх детальніше.

1. Для започаткування функціонування та подальшого розвитку систем кібербезпеки, необхідно розуміти, в якому середовищі вони функціонують. Тут варто зважати на те, що деякі системи слугують забезпеченню відповідних результатів на організаційному рівні, а інші призначені для використання на регіональному або міжнародному рівні. Скажімо, на організаційному рівні ці системи можуть бути належним чином запроваджені, покриваючи лише вузьку сферу внутрішньоорганізаційних "налаштувань", наприклад, для посилення кіберспроможності організації або захисту критичної інформаційної інфраструктури.

Тобто, зовнішнє середовище систем кібербезпеки можна поділити на три рівні: організаційний; регіональний; міжнародний.

Організаційний рівень, як правило, стосується підвищення безпекового потенціалу організації, тоді як інші два мають на меті забезпечення позитивної взаємозалежності різних суб'єктів у сфері кібербезпеки. При цьому організаційна система може використовуватися як система, що доповнює системи вищого рівня, тому організація може також впроваджувати ще одну систему високого рівня поряд із системою організаційного типу [8]. У той же час міжнародні системи, підкреслюючи важливість позитивної взаємозалежності, що має характер кооперації, сприяє встановленню співпраці будь-яких організацій і структур, що мають аналогічні інтереси.

2. Цифровізація роботи органів соціальної сфери не тільки зробила доступ до послуг більш ефективним і зручним для населення, але й привела до підвищення ефективності діяльності цих структур. Зокрема, це досягається впровадженням електронного документообігу, який дає змогу зменшити управлінські ланки без втрати керованості, скоротити час, який працівники витрачають на виконання дрібних завдань та пошук інформації, а також автоматизацією основних бюрократичних процедур.

Дослідники підрахували, що цифрові технології мають потенціал заощадити від 46,2 % до 66,2 % робочого часу [5, с. 59]. Створюючи єдину систему електронної взаємодії всіх органів соціальної сфери, можна зробити роботу окремих підрозділів і всієї структури більш узгодженою [5, с. 71].

Прикладами підвищення загальної ефективності діяльності органів соціальної сфери при використанні інформаційно-комунікативних технологій є створення електронних порталів, що надають адміністративні послуги соціального характеру, відповідних чат-ботів, веб-сайтів органів соціальної сфери, на яких громадяни мають змогу знайти необхідну їм актуальну інформацію. Це також забезпечує прозорість даних щодо діяльності цих суб'єктів. Певні вимоги стосуються розробки веб-сайтів для органів соціальної сфери, щодо гарантування кібербезпеки користувачам, стосовно надання загальної інформації: виду діяльності, включаючи нормотворчі процедури, тексти звернень/промов керівників, технологічні карти надання послуг, статистичну інформацію, зразки документів, години роботи, контакти тощо.

Нині органи соціальної сфери мають значну присутність на різних платформах соціальних мереж. Однак це не скасовує існування конфіденційної інформації в роботі цих установ. До такої інформації належать персональні дані та інша конфіденційна інформація, яка регулюється законодавчими актами та не підлягає розповсюдженню.

3. У роботі з системою кібербезпеки можна виокремити два види заохочувальних дій. Дії першого виду спираються на співпрацю з іншими акторами (зовнішня стратегія), в той час як дії другого виду спрямовані на збільшення кіберпотенціалу певної організації, інституції, структури тощо (внутрішня стратегія). Дії першого виду сприяють співпраці між різними акторами в кіберпросторі, посилюють їхню позитивну взаємозалежність. Основна ідея, закладена в основу цих дій, полягає у тому, що кібербезпека є загальною відповідальністю, а проблеми, що виникають, пов'язані зі взаємозалежностями всіх зацікавлених сторін у кіберпросторі [14; 17; 20]. Тому гарантування кібербезпеки не є виключною відповідальністю однієї організації, натомість, воно має стати загальною справою і, як наслідок, потребує партнерства між зацікавленими сторонами [33].

У свою чергу, другий вид заохочувальних дій підтримує внутрішні процеси та сприяє внутрішньому зміцненню організації через створення або збільшення власної кіберзахищенності. У той час як заохочувальні зовнішні дії спрямовані на спільну боротьбу з кіберзагрозами, для організації також важливо мати

достатню кіберспроможність, щоб бути надійним та сильним самостійним актором. Наприклад, деякі системи кібербезпеки, такі як Oxford University CMM та система NIST, виступають за посилення організаційного потенціалу, наприклад, шляхом нарощення потенціалу людських ресурсів, укріплення критично важливих інформаційних інфраструктур та зміцнення внутрішніх систем (тобто нормативних актів, правил та організаційної структури) [8].

4. Цифровізація сприяє створенню більш ефективних та прозорих каналів комунікації між органами соціальної сфери та громадянами, що включає створення системи зворотного зв'язку, дозволяючи інститутам громадянського суспільства та окремим громадянам надавати свій внесок до спільної мети – соціального добробуту (що актуальне не лише для вразливих верств населення, а й для волонтерських організацій, які прагнуть допомагати людям). Завдяки цьому доступність і ефективність значно покращуються, оскільки будь-хто може залишити коментар, поставити запитання чи подати апеляцію. Хоча доступність інформації та можливість швидкого звернення за допомогою є корисними для громадян, це не обов'язково гарантує, що діяльність органів соціальної сфери стане ефективнішою. Наприклад, звертаючись за соціальною допомогою до певного органу, можна зіткнутися з "круговим циклом" бюрократії, коли управління може перенаправити цифрову заявку громадянина в інше управління або відповісти загальними фразами.

5. Одним із шляхів вирішення суспільно значущих питань є формування електронних майданчиків для взаємодії громадянського суспільства та органів соціальної сфери, такі платформи переважно використовують технологію краудсорсингу. Наприклад, можна згадати пандемійний 2020 р., коли ще більше підвищилась потреба в оперативному зв'язку між органами соціального захисту та громадськістю. У Республіці Корея ще у грудні 2019 р. була створена інтерактивна та оновлювана сторінка, на якій можна було побачити 18 перших зафіксованих у Сеулі випадків захворювання, а також перелік місць, які відвідали хворі. Цифрові служби місцевої влади з'ясували високопріоритетні випадки та відстежили пересування людей, використовуючи інструменти Web 2.0 – дані з мобільних базових станцій та транзакції пластикових банківських карток [18].

Використання таких платформ дає численні позитивні результати, зокрема підвищення прозорості дій органів соціальної сфери, безпосереднє спілкування влади з громадянським суспільством, краще розуміння потреб громадян. Крім того, ці платформи допомагають вирішувати наявні проблеми громадян, люди усвідомлюють роль громадянського суспільства у впливі на прийняття рішень щодо власного добробуту.

В Україні перші кроки щодо цифровізації соціальної сфери було зроблено в рамках проєкту "Удосконалення системи соціальної допомоги" за підтримки Світового банку (2014 р.), метою якого було розроблення Єдиної інформаційно-аналітичної системи соціального захисту населення (далі ЄІАССЗН) [9]. Створення єдиного інформаційного простору соціальної сфери суттєво полегшує оформлення всіх видів соціальної допомоги і пільг, оскільки людині для отримання допомоги потрібно буде надати тільки паспорт, а решту необхідної документації фахівці соціальної сфери зможуть отримати за допомогою нової експериментальної системи [4]. Прагнення розробити уніфіковану базу даних про ЄІАССЗН відповідає основним засадам побудови цифрової економіки як складної екосистеми взаємопов'язаних інформаційних і комунікаційних технологій, що ґрунтується на опрацюванні "великих даних", які забезпечені складним аналітичним інструментарієм [24]. Однак реалізації цього проєкту тоді не відбулося.

Наступним етапом стало підписання нової угоди щодо виконання проєкту "Модернізація системи соціальної підтримки населення України" в контексті сприяння проведенню соціальних реформ, спрямованих на зменшення рівня бідності та підвищення соціальної захищеності найбільш уразливих верств населення. З метою ефективного технічного наповнення ЄІАССЗН виконання проєкту передбачено у три етапи: забезпечення централізації інформаційних систем соціальної сфери; побудова системи обміну даними між інформаційними системами; запровадження механізму онлайн верифікації та аутентифікації громадян, контроль інформаційної системи Міністерством соціальної політики України (далі – МСП) та запровадження верифікації даних.

Важливим кроком у цьому напрямку стало ухвалення урядом рішення про створення Єдиної інформаційно-аналітичної системи управління соціальною підтримкою населення України (E-SOCIAL), Положення про зазначену систему та Положення про Єдиний державний реєстр соціальної сфери (Постанова КМУ № 676 від 17.07.2019) [3]. Відтак, МСП взяло на себе зобов'язання забезпечити:

– створення E-SOCIAL, яка базується на використанні прикладного програмного забезпечення рівня Enterprise із гарантуванням доступу користувачів до прикладних задач через вебінтерфейс;

– наповнення до 30 вересня 2020 р. E-SOCIAL інформацією, яка наявна в інших інформаційних системах, що використовують структурні підрозділи з питань соціального захисту населення;

– використання з 1 жовтня 2020 р. E-SOCIAL при наданні, призначенні та виплаті соціальної допомоги населенню України.

Зараз на базі E-SOCIAL та ЄІАССЗН створена Єдина інформаційна система соціальної сфери (далі – ЄІССС), на якій впроваджено 17 видів допомог, системою користуються в усіх регіонах України, де кількість користувачів – фахівців соціальної сфери – вже перетнула позначку 15 тисяч [7]. Розвиток Єдиної інформаційної системи соціальної сфери триває, враховуючи нові потреби та виклики.

У жовтні 2024 р. Верховна Рада України підтримала у першому читанні законопроєкт

№ 11377, який розробило МСП [11]. Його прийняття дозволить розбудовувати ЄІССС відповідно до принципів:

1) стандартизації даних: ЄІССС допоможе впровадити єдині стандарти для збору та обробки даних, що відповідають європейським нормам. Це полегшить обмін інформацією між державними установами та органами ЄС.

2) прозорості та підзвітності: система забезпечить прозорість у витрачанні бюджетних коштів на соціальні програми, що надасть громадянам можливість легше контролювати діяльність держави.

3) покращення якості соціальних послуг: завдяки інтеграції даних різних установ, соціальні послуги стануть ще більш доступними та якісними.

4) адаптації до європейських стандартів: розбудова системи враховуватиме вимоги ЄС щодо захисту даних та прав людини, а отже сприятиме кращій адаптації українського законодавства до європейських стандартів.

5) можливості моніторингу та оцінки: система дозволить ефективно моніторити соціальну політику та оцінювати її вплив, що допоможе в ухваленні рішень на всіх рівнях.

6) співпраці з міжнародними партнерами: Єдина система створить платформу для співпраці з міжнародними організаціями та фондами, що працюють у соціальній сфері, залучаючи додаткові ресурси та експертизу.

Усі вищенаведені заходи щодо цифровізації вітчизняної соціальної сфери стосуються, насамперед, тих установ, які виконують управлінські й адміністративні функції (міністерство, управління). Фактично в цих структурах: було проведено модернізацію комп'ютерного устаткування та програмного забезпечення; використовується електронний документообіг (як в середині установ, так і з іншими організаціями); пріоритетності набуває кібербезпека і на перший план виходить захист персональних даних клієнтів, як результат, використовуються захищені канали передачі даних.

Практична реалізація цих проєктів і завдань дасть змогу органам соціальної сфери базового рівня гарантувати населенню належні умови щодо призначення, нарахування та отримання соціальних виплат, пільг, соціальних послуг чи житлових субсидій. Більше того, автоматизація окреслених процесів сприятиме підвищенню ефективності діяльності державних органів у сфері соціального захисту та забезпечення населення, запобіганню зловживанням під час надання соціальних послуг та адміністративних послуг соціального характеру, а також покращенню рівня адресності надання соціальної допомоги та ефективності використання бюджетних коштів [1].

Таким чином, основними напрямками застосування інформаційно-комунікаційних технологій в соціальній сфері є:

– автоматизація процесів, що включає обробку звернень громадян в електронному вигляді, автоматичний розрахунок соціальних виплат, ведення електронних реєстрів;

– персоналізація соціальних послуг, яка включає створення індивідуальних планів соціальної підтримки та надання цільової інформації про соціальні послуги;

– покращення взаємодії з громадянами, тобто створення електронних кабінетів громадян, надання можливості отримувати соціальні послуги та адміністративні послуги соціального характеру онлайн;

– аналіз даних, що включає виявлення трендів та закономірностей в соціальній сфері і оптимізацію надання послуг на основі цих даних.

Спираючись на наукові джерела [4; 6; 12] розглянемо основні теоретичні підходи до цифровізації соціальної сфери:

– системний підхід: розглядає соціальну сферу як складну систему, де інформаційно-комунікаційні технології є інструментом для оптимізації взаємодії між різними елементами цієї системи. Дозволяє моделювати та прогнозувати наслідки впровадження нових технологій. Сприяє створенню єдиної інформаційної системи соціальної сфери. Його метою є підвищення ефективності і якості надання соціальних послуг та адміністративних послуг соціального характеру.

– гуманітарний підхід: акцентує увагу на людині як головному бенефіціарі послуг соціальної сфери. Передбачає використання інформаційно-комунікаційних технологій для персоналізації соціального захисту, підвищення його доступності та зручності для громадян. Наголошує на необхідності збереження конфіденційності персональних даних.

– економічний підхід: розглядає інформаційно-комунікаційні технології як інструмент для підвищення ефективності використання бюджетних коштів. Дозволяє оптимізувати процеси організації соціального захисту, зменшити адміністративні бар'єри та підвищити прозорість використання бюджетних коштів.

– інформаційний підхід: підкреслює важливість інформації як ресурсу, що потребує ефективного управління та захисту. Наголошує на важливості врахування соціального контексту при впровадженні цифровізації. Мета – створити технології, які відповідають потребам і можливостям користувачів.

– правовий підхід: визначає правові основи використання інформаційно-комунікаційних технологій у соціальній сфері. Регулює питання захисту персональних даних, електронного документообігу, відповідальності за порушення законодавства в цій сфері.

Не зважаючи на наявність значної кількості підходів до цифровізації соціальної сфери, основною метою запровадження інформаційно-комунікаційних технологій у соціальній сфері є забезпечення ефективного використання наявних ресурсів у рамках:

– гарантування реалізації основних прав і свобод громадян;

– надання соціальної допомоги та соціального захисту особам, які опинилися у складній життєвій ситуації;

– поширення у соціумі знань і формування навичок з профілактики соціально небезпечного становища і взаємодопомоги;

– підтримки прийняття ефективних управлінських рішень, спрямованих на підвищення результативності соціальних послуг та адміністративних послуг соціального характеру.

Цифровізація соціальної сфери має відповідати низці принципів, серед яких безпека посідає чільне місце [13]:

– інклюзивність: засоби цифровізації мають бути доступними для всіх категорій населення, включаючи людей з інвалідністю;

– конфіденційність: захист персональних даних є одним з пріоритетів;

– безпека: інформаційні системи мають бути захищені від кібератак та інших загроз;

– ефективність: цифровізація повинна підвищувати ефективність соціального захисту;

– прозорість: процеси, пов'язані з використанням цифрових інструментів, мають бути прозорими для всіх зацікавлених сторін;

– якість: цифровізація повинна забезпечувати високу якість наданих послуг.

Застосування інформаційно-комунікативних технологій у соціальній сфері гарантує: автоматизацію рутинних процесів (обробка заявок, розрахунок виплат тощо), створення електронних баз даних (зберігання інформації про клієнтів, їхні потреби та надані послуги), розробку мобільних додатків (надання соціальних послуг онлайн, отримання інформації про програми підтримки), використання аналітики даних (для прийняття обґрунтованих рішень та прогнозування потреб), створення онлайн-платформ для взаємодії (соціальні працівники, клієнти, волонтери можуть спілкуватися та співпрацювати в онлайн-режимі) [13]. Загалом, як наголошують А. Крисоватий, А. Луцик та Н. Синютка, існуюча в Україні система електронного урядування полегшує збір та обмін інформацією шляхом автоматизації процесів реєстрації, обміну інформацією та покращення надання державних послуг, у тому числі і в соціальній сфері [21].

Отже, застосування інформаційно-комунікативних технологій у соціальній сфері є необхідним кроком для підвищення ефективності та якості надання соціальних послуг та адміністративних послуг соціального характеру. Однак, для успішної реалізації цього потенціалу необхідно враховувати як безпекові й технічні аспекти, так і соціальні, економічні та правові. Нижче ми зосередимось саме на безпекових аспектах.

Інформаційне суспільство зосереджує увагу на доступі до публічної інформації. Передача інформації між адресатом та одержувачем, яка відбувається на макрорівні (у тому числі в соціальній сфері), є дуже динамічною та включає як публічну інформацію, так і персональні дані зокрема, конфіденційні. Першочерговим завданням адміністраторів веб-сайтів та порталів є аналіз потенційних кіберзагроз, чітко визначаючи стандарти захисту кіберпростору від кібератак. П. Гаврисяк справедливо зазначає, що "стратегії безпеки для веб-сервісів ... повинні постійно переглядатися та оновлюватися" [19, с. 150]. Створення умов, які забезпечують безперебійний доступ до публічної інформації, неможливе без розробки та впровадження оптимальних правових норм і визначення низки технічних вимог до безпеки мереж та інформаційних систем. утім, варто пам'ятати, що право доступу до публічної інформації, яке закріплено Законом України "Про доступ до публічної інформації", є фундаментальним правом особи.

Системи, в яких обробляється публічна інформація, є потенційними джерелами кібератак, а з огляду на різноманітність методів кіберзлочинців, питання кібербезпеки у першу чергу слід розглядати в правовому та технічному контексті. Варто також зважати на те, які дії повинні вживати адміністратори веб-сайтів та державні установи для гарантування кібербезпеки. Зауважимо, що загальний та широко вживаний термін "кібербезпека" охоплює різні питання, які можуть стосуватися технологій, суспільства та політики.

Через відсутність чіткого визначення цього терміну багато явищ, що виникають у нових технологіях, називаються з префіксом "кібер". Тому такі терміни, як "кібератака" або "кібертероризм", часто використовуються як взаємозамінні, що призводить до численних помилкових уявлень щодо ідеї кібербезпеки. Більше того, це дуже складний термін, який може використовуватися в різних сферах, і неможливо віднести його до однієї галузі.

Спроби охарактеризувати концепцію кібербезпеки часто відображають постійні дебати щодо прямої ролі уряду в цьому питанні, способів заохочення або примусу приватного сектору до співпраці та інструментів, які можуть гарантувати належний рівень безпеки інформаційних мереж. Індивідуальний підхід кожного автора та умови кіберсередовища відіграють важливу роль у визначенні кібербезпеки [22]. Іншим важливим фактором є постійний технічний прогрес, який сприяє поширенню цифровізації та вимагає гарантування її безпечного використання. Таким чином, цифровий розвиток створює нові ситуації та відносини, які впливають на інтерпретацію процесів, що відбуваються в рамках кібербезпеки.

Визначення поняття кібербезпеки часто залежить від суб'єкта, для якого існують певне середовище та конкретні загрози, що базово входять до такого визначення. Саме визначення є принцивовим для розуміння того, які заходи необхідно вжити організації для захисту інформації та інфраструктури. У спробах визначити це поняття можна виокремити два основні підходи.

Перший стосується технологій, програмного забезпечення та індивідуальних навичок, що застосовуються для зниження ризиків, що виникають внаслідок передачі та зберігання даних онлайн, таких як технології шифрування, антивірусне програмне забезпечення та навчання персоналу [16; 32].

Слід зазначити, що концепція кібербезпеки може бути недостатньо чіткою, якщо розглядати її виключно як реакцію органів публічного управління

на технічні проблеми у сфері безпеки [25]. Вжиті заходи виходять далеко за рамки заходів фізичної безпеки та окреслюють цілі для багатьох сфер соціального та політичного життя [25; 31]. Однією з причин розширення сфери застосування цієї концепції за межі технічних аспектів є розсилка незаконного та шкідливого контенту, який впливає на комп'ютерні мережі та системи, може негативно впливати на політичне і соціальне життя країни (особливо, якщо проти країни ведеться гібридна війна).

Згідно з другим підходом, виключно зміни у військових технологіях є традиційним елементом, що використовується для визначення кібербезпеки [27; 29]. На початку XXI ст. спостерігалося зростання кількості міжнародних конфліктів та суперечок, майже в кожному випадку пов'язаних з цифровими технологіями, що використовували "шкідливе програмне забезпечення" для ослаблення критичної інфраструктури противника або ж для несанкціонованого доступу до інформації. Отже, акцентування уваги на негативних результатах використаної технології є типовою рисою більшості визначень кібербезпеки та механізмів безпеки, що впроваджуються урядами для захисту своїх країн від кібератак. Утім, в межах згаданої вище гібридної війни, мова може йти скоріше про розповсюдження неправдивої інформації, яка здатна нанести шкоду державі, суспільству та окремим громадянам. Наприклад, запуск від імені Мінсоцполітики інформації про скасування низки соціальних виплат та дотримання державних соціальних гарантій в умовах воєнного стану.

З моменту усвідомлення того, що кібератаки виходять далеко за межі кіберпростору та впливають на повсякденне життя громадян, питання забезпечення захисту та стабільності набуло політичного забарвлення. Кіберзагрози також стали значною проблемою, оскільки вони можуть впливати на інфраструктуру країни та спричиняти суттєві витрати на превентивні заходи. Це означає, що зобов'язання забезпечувати захист від таких загроз не може залишитися непоміченим або ігноруватися органами публічного управління, оскільки бездіяльність вплине на переважну більшість суспільства, у першу чергу на соціально вразливі верстви населення.

Тобто органи публічного управління мають відповіді на такі питання, як:

– наскільки високим має бути обсяг коштів, призначених для покриття витрат на кібербезпеку?

– які превентивні дії слід вжити для запобігання можливим загрозам?

– як зберегти пропорції та належний обсяг реагування на кібератаку?

Це лише деякі з багатьох питань, на які необхідно звернути увагу в офіційних стратегічних документах щодо національної безпеки. Тому наразі неможливо обговорювати питання кібербезпеки, не враховуючи політичні аспекти, і пошук рішень вищезазначених проблем є справжнім викликом для будь-якого уряду.

Наразі багато суспільств обмінюються персональними даними за допомогою цифрових технологій. Однак захист даних – це ізоляція даних, а також правила та методи їх передачі та використання. Таким чином, кібербезпека також сприймається як "концепція, пов'язана з діями, що вживаються державними та приватними суб'єктами для забезпечення безпеки комунікацій та онлайн-ресурсів" [28, с. 80].

Хоча захист даних важливий для стабільного розвитку держави, кібербезпека – це набагато ширше явище, що охоплює численні питання, які не пов'язані безпосередньо з інформаційними технологіями та комп'ютерними послугами [25]. У літературі з цієї теми можна знайти, що сучасні умови життя багатьох людей залежать від програм та послуг, заснованих на аналізі даних [15]. Численні організації збирають, обробляють та аналізують великий обсяг даних для надання персоналізованих послуг або розробки більш ефективних систем у різних секторах, таких як охорона здоров'я, соціальне обслуговування, громадський транспорт та страхування. Таким чином, організації також можуть впливати на низку альтернатив, доступних для окремої особи. У цьому контексті захист даних набуває особливої актуальності, оскільки він тісно пов'язаний з демократичними цінностями, пов'язаними з правом особи на самовизначення та вибором медіаінформації. Отже, кібербезпека являє собою право особи вирішувати (не лише для себе), щодо даних, які вона хоче передавати, кому та чому. Таким чином, захист персональних даних як індивідуальна мета може конкурувати з колективними інтересами суспільства в таких сферах, як громадський порядок чи безпека.

Право на приватність як одне з основних прав людини має захищати особу від втручання державних органів. Однак за обставин, коли кібертехнології дозволяють зберігати великі дані, приватні постачальники послуг, які обробляють ці дані, є особливо важливими для політики кібербезпеки, оскільки вони можуть розголошувати унікальну інформацію про своїх користувачів. Тобто дедалі більше захист персональних даних від несанкціонованого доступу стає політичним питанням і часто є предметом політичних дебатів.

Не менш важливим питанням є визначення сфери кіберзагроз, які сьогодні можуть порушувати доступ та обробку даних в умовах цифровізації. Враховуючи різноманітний характер кібератак (шкідливе програмне забезпечення, перехоплення передачі з'єднань, незаконна обробка, несанкціонований доступ тощо), політика кібербезпеки повинна визначати правові, організаційні та соціально-економічні умови, пов'язані із забезпеченням безпеки на усіх рівнях. Як наголошує А. Монарха-Матлак, "роздуми про майбутнє доступу до публічної інформації включають міркування не лише економічного чи політичного характеру, а й, перш за все, технічного характеру" [23, с. 17].

У першу чергу, політика кібербезпеки повинна чітко визначати, як класифікувати небезпечні інциденти. Водночас вона повинна вказувати, хто і якою мірою (наприклад, адміністратор веб-сайту)

відповідає за вжиття таких заходів, як: початкова оцінка інциденту (тип, масштаб та потенційні наслідки кіберзагрози) та вжиття заходів щодо інциденту (вжиття подальших дій після того, як інцидент фактично стався). Питання зміцнення цифрових компетенцій серед суб'єктів, які обробляють та використовують інформацію, розміщену в Інтернеті, також є надзвичайно важливим [26]. Вищезазначене, безумовно, має відповідати головній меті Закону України "Про основні засади забезпечення кібербезпеки України" [10], а саме: підвищити рівень стійкості до кіберзагроз та підвищити рівень захисту інформації в державному, військовому та приватному секторах, а також сприяти поширенню знань та передового досвіду, що дозволяє громадянам краще захищати свої дані. Хоча користувачі мобільних пристроїв можуть самі піддавати ризику себе і свої дані, це загалом є організаційною проблемою, оскільки установи публічного сектора повинні розширити свою стратегію кібербезпеки, відповідно включивши до неї питання захисту інформації мобільних пристроїв, доступ до якої можна отримати через такі пристрої [8]. Але складність поширення кібербезпеки на різні мобільні пристрої, ймовірно, зростатиме, оскільки наслідки зростання мобільності для публічного сектора є більшими, ніж просто захист окремих телефонів і управління процедурами резервного копіювання. Перехід до мобільності зрештою буде означати, що ми всі постійно будемо, так би мовити, "на зв'язку", і подібна ситуація все частіше буде зустрічатись в усьому світі. Тому організації соціальної сфери мають співпрацювати з операторами мереж та послуг для розробки безпечної архітектури, забезпечення можливості моніторингу і фільтрації трафіка, а також постійного вдосконалення політик і керівних принципів управління всередині організацій.

Висновки. За останнє десятиліття багато досліджень було присвячено питанню кібербезпеки як міждисциплінарному явищу, важливому для аналізу соціально-політичного простору суспільного життя. Такі дослідження розвиваються через зміни в суспільному середовищі, що пропонує нові емпіричні дані для подальших досліджень. Нові напрямки досліджень також розкривають ті аспекти кібербезпеки, які раніше залишалися непоміченими як дослідниками, так і спостерігачами, але вони стали об'єктом уваги як потенційна загроза під час гібридної війни.

У цьому контексті зв'язки між технологіями, наукою та практикою публічного управління є особливо важливими та найчастіше зводяться до того, як державні суб'єкти, які беруть участь у цих сферах, формулюють свої цілі, виконують свої завдання, як вони сприймають свої ролі та яку діяльність вони здійснюють стосовно кібербезпеки на національному та локальному рівнях у всіх сферах, включаючи соціальну.

Таким чином, одним з ключових питань політики кібербезпеки, що стоять перед публічними органами при розгляді рішень про те, як краще за все впровадити соціальні мережі в діяльність публічних організацій, є питання забезпечення належного балансу між управлінням ризиками і створенням дійсно відкритого уряду. Адже захист персональних даних як індивідуальна мета може конкурувати з колективними інтересами суспільства в таких сферах, як громадський порядок чи безпека, що ускладнюється існуванням природного протиріччя між характеристиками відкритого уряду, – відкритими даними, відкритим доступом, прозорістю і підзвітністю, – і проблемами гарантування безпеки.

Список джерел інформації

1. Бірнс Т. (2024). *Єдина інформаційна система соціальної сфери (ЄІССС). Зміцнення інфраструктури соцзахисту в Україні в умовах кризи у 2023.* Технічна допомога у сфері соцзахисту, поради та ресурси, LLC DAI Global UK, Велика Британія. Retrieved from https://medirent.ua/images/2024/STAAR_2024.pdf

2. Васильковський О.Т. (2022). Фактори, що детермінують взаємодію органів публічного управління з громадськістю у цифровій реальності. *Наукові перспективи*. № 9 (27). С. 46 – 57. DOI https://doi.org/10.52058/2708-7530-2022-9(27)-46-56

3. Дакалюк О. (2020). Інформаційно-комунікаційні технології як засіб активізації самостійної роботи студентів в умовах дистанційного навчання. *Modern information technologies and innovation methodologies of education in professional training methodology theory experience problems*. С. 35 – 42. DOI https://doi.org/10.31652/2412-1142-2020-58-35-42

4. Дітковська Л. (2013). Місце інформаційно-комунікаційних технологій у професійній діяльності соціальних працівників. *Збірник наукових праць ХІСТ Університету "Україна"*. № 2 (8). С. 78 – 82.

5. *Електронне урядування* : підручник. (2014). Авт. кол. : В.П. Горбулін, Н.В. Грицяк, А.І. Семенченко, О.В. Карпенко та ін.; за заг. ред. проф. Ю.В. Ковбасюка ; наук. ред. проф. Н.В. Грицяк, проф. А.І. Семенченка. К. : НАДУ. 352 с.

6. *Інформаційні системи та технології* : навчальний посібник. (2020). Х. : ХНАУ ім. В.В. Докучаєва. 207 с.

7. ЄІССС. Retrieved from https://www.msp.gov.ua/e-servisy/yeisss

8. Котух Є.В. (2021). *Кібербезпека у публічному секторі* : моногр. Х. : Вид-во ХарРІ НАДУ "Магістр". 272 с.

9. Мінсоцполітики: Світовий банк виділив Україні кошти на модернізацію системи соціальної допомоги. Retrieved from https://www.kmu.gov.ua/ news/247437750

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (в редакції від 20.04.2025). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text

11. Про прийняття за основу проєкту Закону України про Єдину інформаційну систему соціальної сфери : Постанова Верховної Ради України. Retrieved from https://zakon.rada.gov.ua/laws/show/4035-IX

12. Руденко Л.А. (2017). Самоосвіта і саморозвиток майбутніх фахівців соціального захисту в інформаційному суспільстві. *Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми* : зб. наук. пр. № 49. С. 157 – 160.

13. Ющенко Н., Ковтун М. (2019). Електронне урядування в Україні: стан та перспективи розвитку. *Причорноморські економічні студії : економічн. наук.-практ. журнал*. № 38. Retrieved from http://bses.in.ua/journals/2019/38_1_2019/31.pdf

14. BSA Global *Cybersecurity Framework*. (2010). Washington, DC, USA : Business Software Alliance.

15. Cohen J.E. (2013). What privacy is for. *Harvard Law Review*, 126, 1904-1933.

16. Donaldson S.E., Siegel, S., Williams C.K., Aslam A. (2016). *Enterprise cybersecurity*. How to build a successful cyberdefense program against advanced threats. Apress, Berkeley, CA., pp. 213 – 229.

17. European Commission. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels. DOI : 10.4271/2010-01-1021.

18. Embassy of the Republic of Korea to the Kingdom of the Netherlands. Korea's Fight against COVID-19. Retrieved from http://overseas.mofa.go.kr/nl-en/brd/m_6971/view.do?seq=761546

19. Gawrysiak Piotr. (2012). Portale internetowe – zagrozenia realne i pozorne. *Prawno-informatyczne problemy sieci, portali i e-uslug.* Edited by Grazyna Szpor, and Wojciech R. Wiewiorowski. P. 145 – 151.

20. ISO/IEC. (2012). Information Technology – Security Techniques – Guidelines for Cybersecurity. Geneva : ISO/IEC.

21. Krysovatyi A., Lutsyk A., Synyutka N. (2019). Influence of time lags on the efficiency of fiscal policy in Ukraine. *9th International conference on advanced computer information technologies*, ACIT 2019 – Proceedings. art. no. 8780059. P. 380 – 383.

22. Lindstrom G., Luiijf E. (2012). Political Aims & Policy Methods. In A. Klimburg, (Ed.), *National cybersecurity framework manual*, pp. 45 – 47.

23. Monarcha-Matlak Aleksandra. (2008). *Obowiązki administracji w komunikacji elektronicznej.* Warszawa : Oficyna a Wolters Kluwer business. Retrieved from https://www.nexto.pl/upload/publisher/Wolterskluwer/public/obowiazki_admin_w_komun%20demo.pdf?srsltid=AfmBOorh4zLQQeUfdgnd2s45u-ninXGTiXzR3PzALxzrzNXVBWv_qeMs

24. Monino J.-L. (2016). Data value, big data analytics and decision-making. *Journal of Knowledge Economy*. P. 1 – 12. DOI https://doi. org/10.1007/s13132–016–0396–2

25. Nissenbaum H. (2015). Where computer security meets national security. *Ethics and Information Technology*, 7 (2), 61 – 73.

26. Pawel Switał, Dominika Skoczylas. (2024) The information sphere in the age of cyberthreats. Disinformation and cybersecurity. *Teka Komisji Prawniczej*, vol. XVII, no. 1, pp. 257 – 271. DOI https://doi.org/10.32084/tkp.5812

27. Rid T. (2012). Cyber war will not take place. *The Journal of Strategic Studies*, 35 (1), 5 – 32.

28. Sienkiewicz P., Swieboda H. (2009). Sieci teleinformatyczne jako instrument panstwa – zjawisko walki informacyjnej. In M. Madej, M. Terlikowski, (Eds.), *Bezpieczenstwo teleinformatyczne panstwa*. Warszawa : Polski Instytut Spraw Midzynarodowych. 162 p.

29. Stone J. (2013). Cyber war will take place. *The Journal of Strategic Studies*, 36 (1), 101 – 108.

30. Timmers P (2019). Challenged by Digital Sovereignty. *Journal of Internet Law*, 23 (6), 1 – 20.

31. Walker J., Melinda C. (2011). Genealogies of resilience. From systems ecology to the political economy of crisis adaption. *Security Dialogue*, 42 (2), 143 – 160.

32. Weber R.H. (2018). Privacy and security in the IoT – Legal issues. In A. Moallem, (Ed.), *Human-Computer Interaction and Cybersecurity Handbook*. CRC Press, pp. 306 – 308.

33. WEF (2012). Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience". Geneva, Switzerland: World Economic Forum (WEF). Retrieved from https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience

References (transliterated)

1. Birns T. (2024). Yedyna informatsiina systema sotsialnoi sfery (YeISSS). Zmitsnennia infrastruktury sotszakhystu v Ukraini v umovakh kryzy u 2023. Tekhnichna dopomoha u sferi sotszakhystu, porady ta resursy, LLC DAI Global UK, Velyka Brytaniia. Retrieved from https://medirent.ua/images/2024/STAAR_2024.pdf

2. Vasylkovskyi O.T. (2022). Faktory, shcho determinuiut vzaiemodiiu orhaniv publichnoho upravlinnia z hromadskistiu u tsyfrovii realnosti. Naukovi perspektyvy. № 9 (27). S. 46 – 57. DOI https://doi.org/10.52058/2708-7530-2022-9(27)-46-56

3. Dakaliuk O. (2020). Informatsiino-komunikatsiini tekhnolohii yak zasib aktyvizatsii samostiinoi roboty studentiv v umovakh dystantsiinoho navchannia. Modern information technologies and innovation methodologies of education in professional training methodology theory experience problems. S. 35 – 42. DOI https://doi.org/10.31652/2412-1142-2020-58-35-42

4. Ditkovska L. (2013). Mistse informatsiino-komunikatsiinykh tekhnolohii u profesiinii diialnosti sotsialnykh pratsivnykiv. Zbirnyk naukovykh prats KhIST Universytetu "Ukraina". № 2 (8). S. 78 – 82.

5. Elektronne uriaduvannia : pidruchnyk. (2014). Avt. kol. : V.P. Horbulin, N.V. Hrytsiak, A.I. Semenchenko, O.V. Karpenko ta in.; za zah. red. prof. Yu.V. Kovbasiuka ; nauk. red. prof. N.V. Hrytsiak, prof. A.I. Semenchenka. K. : NADU. 352 s.

6. Informatsiini systemy ta tekhnolohii : navchalnyi posibnyk. (2020). Kh. : KhNAU im. V.V. Dokuchaieva. 207 s.

7. YeISSS. Retrieved from https://www.msp.gov.ua/e-servisy/yeisss

8. Kotukh Ye.V. (2021). Kiberbezpeka u publichnomu sektori : monohrafiia. Kh. : Vyd-vo KharRI NADU "Mahistr". 272 s.

9. Minsotspolityky: Svitovyi bank vydilyv Ukraini koshty na modernizatsiiu systemy sotsialnoi dopomohy. Retrieved from https://www.kmu.gov.ua/ news/247437750

10. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05.10.2017 № 2163-VIII (v redaktsii vid 20.04.2025). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text

11. Pro pryiniattia za osnovu proiektu Zakonu Ukrainy pro Yedynu informatsiinu systemu sotsialnoi sfery : Postanova Verkhovnoi Rady Ukrainy. Retrieved from https://zakon.rada.gov.ua/laws/show/4035-IX

12. Rudenko L.A. (2017). Samoosvita i samorozvytok maibutnikh fakhivtsiv sotsialnoho zakhystu v informatsiinomu suspilstvi. Suchasni informatsiini tekhnolohii ta innovatsiini metodyky navchannia v pidhotovtsi fakhivtsiv: metodolohiia, teoriia, dosvid, problemy : zb. nauk. pr. № 49. S. 157 – 160.

13. Yushchenko N., Kovtun M. (2019). Elektronne uriaduvannia v Ukraini: stan ta perspektyvy rozvytku. Prychornomorski ekonomichni studii : ekonomichn. nauk.-prakt. zhurnal. № 38. Retrieved from http://bses.in.ua/journals/2019/38_1_2019/31.pdf

14. BSA Global Cybersecurity Framework. (2010). Washington, DC, USA : Business Software Alliance.

15. Cohen J.E. (2013). What privacy is for. Harvard Law Review, 126, 1904-1933.

16. Donaldson S.E., Siegel, S., Williams C.K., Aslam A. (2016). Enterprise cybersecurity. How to build a successful cyberdefense program against advanced threats. Apress, Berkeley, CA., pp. 213 – 229.

17. European Commission. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels. DOI : 10.4271/2010-01-1021.

18. Embassy of the Republic of Korea to the Kingdom of the Netherlands. Korea's Fight against COVID-19.

Retrieved from http://overseas.mofa.go.kr/nl-en/brd/m_6971/view.do?seq=761546

19. Gawrysiak Piotr. (2012). Portale internetowe – zagrozenia realne i pozorne. Prawno-informatyczne problemy sieci, portali i e-uslug. Edited by Grazyna Szpor, and Wojciech R. Wiewiorowski. P. 145 – 151.

20. ISO/IEC. (2012). Information Technology – Security Techniques – Guidelines for Cybersecurity. Geneva : ISO/IEC.

21. Krysovatyi A., Lutsyk A., Synyutka N. (2019). Influence of time lags on the efficiency of fiscal policy in Ukraine. 9th International conference on advanced computer information technologies, ACIT 2019 – Proceedings. art. no. 8780059. P. 380 – 383.

22. Lindstrom G., Luiijf E. (2012). Political Aims & Policy Methods. In A. Klimburg, (Ed.), National cybersecurity framework manual, pp. 45 – 47.

23. Monarcha-Matlak Aleksandra. (2008). Obowiązki administracji w komunikacji elektro- nicznej. Warszawa : Oficyna a Wolters Kluwer business. Retrieved from https://www.nexto.pl/upload/publisher/Wolterskluwer/public/obowiazki_admin_w_komun%20demo.pdf?srsltid=AfmBOorh4zLQQeUfdgnd2s45u-ninXGTiXzR3PzALxzrzNXVBWv_qeMs

24. Monino J.-L. (2016). Data value, big data analytics and decision-making. Journal of Knowledge Economy. P. 1 – 12. DOI https://doi. org/10.1007/s13132–016–0396–2

25. Nissenbaum H. (2015). Where computer security meets national security. Ethics and Information Technology, 7 (2), 61 – 73.

26. Pawel Swital, Dominika Skoczylas. (2024) The information sphere in the age of cyberthreats. Disinformation and cybersecurity. Teka Komisji Prawniczej, vol. XVII, no. 1, pp. 257 – 271. DOI https://doi.org/10.32084/tkp.5812

27. Rid T. (2012). Cyber war will not take place. The Journal of Strategic Studies, 35 (1), 5 – 32.

28. Sienkiewicz P, Swieboda H. (2009). Sieci teleinformatyczne jako instrument panstwa – zjawisko walki informacyjnej. In M. Madej, M. Terlikowski, (Eds.), Bezpieczenstwo teleinformatyczne panstwa. Warszawa : Polski Instytut Spraw Midzynarodowych. 162 p.

29. Stone J. (2013). Cyber war will take place. The Journal of Strategic Studies, 36 (1), 101 – 108.

30. Timmers P (2019). Challenged by Digital Sovereignty. Journal of Internet Law, 23 (6), 1 – 20.

31. Walker J., Melinda C. (2011). Genealogies of resilience. From systems ecology to the political economy of crisis adaption. Security Dialogue, 42 (2), 143 – 160.

32. Weber R.H. (2018). Privacy and security in the IoT – Legal issues. In A. Moallem, (Ed.), Human-Computer Interaction and Cybersecurity Handbook CRC Press, pp. 306 – 308.

33. WEF (2012). Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience". Geneva, Switzerland: World Economic Forum (WEF). Retrieved from https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience

Надійшла (received) 30.05.2025

Відомості про авторів / About the Authors

Грень Лариса Миколаївна (Larysa Hren) – Національний технічний університет «Харківський політехнічний інститут», доктор наук з державного управління, професор, професор кафедри педагогіки та психології управління соціальними системами ім. акад. І.А. Зязюна; Харків, Україна; ORCID: https://orcid.org/0000-0003-4466-6018

Грибко Ольга Владиславівна (Olga Grybko) – Національний технічний університет «Харківський політехнічний інститут», кандидат наук з державного управління, доцент кафедри педагогіки та психології управління соціальними системами ім. акад. І.А. Зязюна; Харків, Україна;
ORCID: https://orcid.org/0000-0003-3227-608X