УДК 347.12
DOI https://doi.org/10.32782/2524-0374/2021-2/25

ДЕЯКІ ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я ПІД ЧАС ПАНДЕМІЇ COVID-19

SOME ISSUES OF PERSONAL DATA PROTECTION IN THE FIELD OF HEALTH DURING THE COVID-19 PANDEMIC

Юніна М.П., к.ю.н., доцент,
доцент кафедри цивільного права та процесу
Дніпропетровський державний університет внутрішніх справ

Лукомська А.А., курсант ІІ курсу факультету підготовки фахівців
для органів досудового розслідування
Дніпропетровський державний університет внутрішніх справ

Стаття присвячена теоретичному обґрунтуванню та дослідженню державних механізмів забезпечення захисту персональних даних у сфері охорони здоров'я під час пандемії COVID-19 і визначення можливих шляхів їх розвитку та вдосконалення. Необхідність вирішення цього питання зумовлена рядом негативних факторів. Так, наприклад, сьогодні в Україні у контексті пандемії вводиться в дію законодавство, яке певним чином порушує права людини. Водночас міжнародні норми про права людини гарантують кожному право на найвищий рівень здоров'я і зобов'язують державу вживати заходів для запобігання загрозам здоров'ю населення і на надання медичної допомоги тим, хто її потребує. Міжнародні стандарти у сфері прав людини також передбачають, що в ситуаціях серйозних загроз для здоров'я населення і надзвичайних станів, які загрожують життю нації, допустимі обмеження певних прав і свобод, якщо такі обмеження вводяться в законному порядку, безумовно необхідні та науково обґрунтовані, а також якщо їх застосування не є довільним або дискримінаційним і обмеженим за часом, якщо дотримується людська гідність, крім того, такі обмеження підлягають контролю і відповідної переслідуваної мети.

Масштаб і гострота пандемії COVID-19 досягають рівня загрози здоров'ю населення, який може виправдовувати обмеження певних прав і свобод. Чинне ж нині національне законодавство України у цій сфері виявилося не готовим до викликів COVID-19 і характеризується відсутністю рівноваги між приватним життям і здоров'ям населення. Саме тому сьогодні однією з головних задач, що потребує негайного вирішення, є створення ефективного механізму захисту персональних даних пацієнтів і посилення відповідальності осіб, винних у такому розголошенні, адже наслідки витоків такої інформації можуть виявитися дуже серйозними для клініки та відповідальних за інцидент співробітників. Порушення безпеки можуть призвести до адміністративної, цивільно-правової, дисциплінарної або навіть кримінальної відповідальності як керівництва клініки, так і її співробітників, винних у цьому.

Ключові слова: COVID-19, сфера охорони здоров'я, персональні данні, обмеження, пацієнт, захист інформації.

The article is devoted to the theoretical substantiation of state mechanisms for ensuring the protection of personal data in the field of health care during the COVID-19 pandemic, and decision of possible ways of their development and perfection.

The necessity of decision of this question is predefined by the row of negative factors. So, for example, today in Ukraine a legislation that violates human rights definitely is put in the context of pandemic in an operation. In the same time international norms about human rights avouch for each a right on the greatest health level and obligate the state to take measure for prevention of threats to the health of population and on the grant of medicare that, who needs her. International standards in area of human rights provide for also, that in the situations of serious threats for the health of population and superexcellences that threaten to life of nation, possible limitations of certain rights and freedoms, if such limitations are entered in the legal order, undoubtedly necessary and scientifically reasonable, and also, if their application is not arbitrary or discriminatory and limit at times, if human dignity sticks to here, in addition such limitations are subject control and corresponding pursued aim.

Scale and sharpness of pandemic of COVID-19 undoubtedly reach level threat to the health of population, that can justify limitation of certain rights and freedoms. A current now national legislation of Ukraine in the field of it is it appeared not ready to the calls of COVID-19 and is characterized an unbalance between private life and health of population. For this reason today one of main tasks, that needs immediate permission, creation of effective mechanism of defence of these personal patients and strengthening of responsibility of persons guilty in such disclosure is. In fact the consequences of sources of such information can appear very serious for a clinic and accountable for an incident employees. Security breaches can result in administrative, civil, disciplinary or even criminal liability as guidance of clinic, and her employees guilty herein.

Key words: COVID-19, healthcare, personal data, restrictions, patient, information protection.

Бізнес і держструктури щодня мають справу з величезними обсягами персональних даних: вони «знають» наші імена та прізвища, дати народження й адреси, сімейний стан і соціальний статус, однак особливо гостро питання інформаційної безпеки постає перед медичними установами, адже вони збирають і зберігають персональні дані, вкрай чутливі для будь-якої людини, – результати лабораторних та інструментальних досліджень, діагнози, історії хвороб.

Робота в медичних установах відрізняється низкою особливостей. Клініки зобов'язані зберігати дані про здоров'я кожного пацієнта у вигляді медкарти, і розголошувати їх заборонено за будь-яких умов, тому гостро постає проблема можливих витоків інформації.

Питанням захисту персональних даних присвячено багато різнопланових праць як зарубіжних, так і вітчизняних дослідників. Так, серед вітчизняних варто виділити праці А. Анісимова, І. Арістової, О. Баранова, Ю. Батурина, І. Бачила, З. Богатиренко, І. Бочкарьова, В. Брижка, Н. Грицяк, В. Дзюндзюка, А. Марущака, О. Жуковської, Є. Захарова, В. Іванського, І. Кісельова, М. Лапчинського, В. Ліпкана, А. Левенчука, А. Лушнікова, М. Лушнікової, І. Маміофа, Р. Марутян, А. Минькова, Є. Муньє, А. Пазюка, А. Семенченка, О. Соколова, О. Сосніна, В. Степанова, Ю. Тихомирова, А. Чернобай, В. Цимбалюка, М. Швеця й ін.

Метою наукової статті є дослідження державних механізмів забезпечення захисту персональних даних у сфері охорони здоров'я під час пандемії COVID-19 і визначення можливих шляхів їх розвитку та вдосконалення.

11 березня 2020 р. Всесвітня організація охорони здоров'я оголосила, що епідемія вірусу COVID-19, який вперше був ідентифікований у грудні 2019 р. в місті Ухань у Китаї, досягла рівня пандемії. Тому ВООЗ закликала держави вжити невідкладних і рішучих заходів, щоб приборкати поширення коронавірусу.

Міжнародні норми про права людини гарантують кожному право на найвищий рівень здоров'я, зобов'язуючи державу вживати заходів для запобігання загрозам здоров'ю населення, і на надання медичної допомоги тим, хто її потребує. Міжнародні стандарти у сфері прав людини також передбачають, що в ситуаціях серйозних загроз для здоров'я населення і надзвичайних станів, що загрожують життю нації, допустимі обмеження певних прав і свобод, якщо такі обмеження вводяться в законному порядку, безумовно необхідні та науково обґрунтовані, а також якщо їх застосування не є довільним або дискримінаційним і обмеженим за часом, якщо дотримується людська гідність, крім того, такі обмеження підлягають контролю і відповідній переслідуваній меті. Масштаб і гострота пандемії COVID-19 безумовно досягають рівня загрози здоров'ю населення, який може виправдовувати обмеження певних прав і свобод.

Боротьба з пандемією COVID-19 розділила світ на два табори. До першого можна віднести Україну разом з іншими країнами, які ввели жорсткий карантин і обмежили свободу пересування громадян, тим самим поставивши економіку на паузу. До другого – держави, котрі пішли шляхом виявлення хворих і тих, хто з ними контактував, за допомогою аналізу персональних даних громадян. Тож виникає питання: хто, як і з яким результатом це робить у світі? І чи є в Україні законодавчі інструменти, які дозволяють збирати та використовувати персональні дані українців з метою стримати пандемію? Відповісти на це питання можна, охарактеризувавши досвід зарубіжних країн. Наприклад, як це зробили в Південній Кореї.

Південна Корея – яскравий приклад того, як можна стримати падіння економіки та поширення вірусу, використовуючи інформаційні технології в роботі з персональними даними громадян. Число інфікованих у країні зросло від кількох десятків до кількох тисяч, досягнувши піку в кінці лютого, але вже до кінця березня статистика показала різке падіння кількості нових випадків [1].

Влада ізолювала пацієнтів, спеціальні державні органи відстежували, тестували тих, хто був у зоні контактів із ними, і застосовували адекватні заходи в кожному конкретному випадку. Крім того, Південна Корея прийняла закони, що дозволяють збирати і публікувати інформацію про пересування хворих, виключаючи можливість їхньої персональної ідентифікації. Для цього йшли в хід записи камер спостереження, історії платежів банківськими картами, дані GPS автомобілів і мобільних пристроїв.

Коли ПЛР-тест пацієнта виявлявся позитивним, жителям району приходили SMS з інформацією про вік і стать інфікованого, а також докладний звіт про його поїздки – види транспорту, координати маршрутів, відвідані публічні місця і навіть те, чи була людина в масці [2].

Також у Південній Кореї розробили веб-сайти і додатки для смартфонів зі збору та відображення подібних даних. Щоденна перевірка таких веб-сайтів стала звичайною частиною життя корейців. Більш того, інфікованих, котрі перебувають на самоізоляції, зобов'язали використовувати спеціальний додаток, яке збирає і миттєво передає дані про локації користувача до контролюючих органів у разі порушення режиму ізоляції [2].

В Україні заяви представників влади засновані на крайнощах – від введення режиму НС з усіма наслідками, що неабияк впливають на українську економіку, до ідеї збирати і поширювати персональні дані хворих та інфікованих за прикладом Південної Кореї.

Наприклад, представниками влади були оголошені такі заяви:

Заява № 1: для контролю за дотриманням умов карантину українська влада звернулася до мобільних операторів і банків за наданням інформації про локації користувачів і їхніх банківських операцій [3].

Згідно з чинними законами мобільні оператори та банки можуть передати органам влади наші персональні дані без нашого відома і згоди, але тільки в разі, якщо йдеться про необхідність проведення слідчих дій у рамках вже відкритого кримінального провадження.

Логічно припустити, що для цього як мінімум повинні мати місце: факт правопорушення; відкрите кримінальне провадження за цим фактом; підозра про причетність відслідковування абонента(-тів), тобто кожного з нас, до скоєння кримінального правопорушення.

Навіть якщо вважати правопорушенням факт недотримання режиму карантину, то згідно з чинним законодавством для більшості з нас це буде адміністративним, а не кримінальним правопорушенням (ст. 44-3 Кодексу про адміністративні правопорушення).

Кримінальна відповідальність передбачена тільки для тих, у чиї службові або професійні обов'язки входить необхідність дотримуватися умов карантину (наприклад, для ресторатів).

Заява № 2: Мінцифра запускає мобільний додаток для контролю за дотриманням карантину або самоізоляції [4].

Дійсно, при завантаженні додатків передплатники погоджуються з умовами їх використання, але такий сценарій передбачає добровільне бажання абонента на використання додатків.

І тут постає запитання. Наприклад, яким чином за відсутності ініціативи з боку абонента використання такого додатка може стати обов'язковим? Законів, які зобов'язали б громадян його встановити і використовувати, в Україні немає. Як бути з тією частиною населення, у якої, в принципі, немає можливості користуватися смартфоном?

Тому залишається тільки закликати власників смартфонів добровільно використовувати такий додаток, сподіваючись на їхню адекватність при оцінці ризиків. Такий додаток вже є, і він використовувався та використовується. Раніше це був додаток «Дій вдома», а зараз «Дія». Розробляла додаток компанія EPAM.

Мінцифри офіційно запустило мобільний додаток для державних послуг «Дія». Його можна скачати в App Store і Google Play. Без проблем у перший же день не обійшлося: користувачі скаржаться на некоректну роботу програми на Android, а деякі хвилюються за безпеку своїх даних.

В EPAM розповідають, що для захисту персональних даних використовували підхід defense-in-depth (система з кількома рівнями безпеки). Також провели ряд тестів, у т. ч. і penetration test (тест на захищеність від проникнення зловмисників).

«Авторизація відбувається через банківські системи, до яких виставлені жорсткі вимоги безпеки. Всі дані користувачів надійно шифруються на смартфоні та зберігаються там виключно в зашифрованому вигляді. На серверній частині ніякі дані користувачів не зберігаються, вони передаються транзитом від реєстру МВС на мобільний додаток», – говорять в EPAM. У зашифрованому вигляді також передається інформація в каналах передачі даних, а на деяких етапах використовується подвійне шифрування. Серверна частина системи розміщена в Україні та розгорнута у «хмарах», які використовуються Мінцифрою для інших своїх сервісів [13].

Заява № 3: Мінцифри звернулося до операторів мобільного зв'язку з проханням надати дані без персональної інформації про абонентів, що повернулися з роумінгу з низки країн із пандемією, починаючи із 17 березня 2020 р. [5].

Ситуація повторюється: без згоди абонента персональні дані можна передавати тільки в рамках кримінального провадження. Плюс до цього, їх можна передавати тільки строго обумовленим законом респондентам: органам досудового розслідування, прокуратурі або судовим органам. Мінцифра, як бачимо, не входить у цей список.

Більш того, заява № 3 в разі її реалізації є для такого мобільного оператора ще й потенційно кримінально караним злочином (ст. 182 Кримінального кодексу України).

До боротьби з пандемією Україні потрібно підходити виважено, щоб одночасно вирішити два завдання – протистояти поширенню вірусу і запобігти колапсу економіки. Не менш важливо не допустити порушення закріплених у Конституції цивільних прав українців. За нинішніх умов слід у короткі терміни доопрацювати законодавство, яке виявилося не готове до викликів COVID-19.

До того ж сьогодні в Україні у контексті пандемії вводиться в дію законодавство, яке, на нашу думку, часто порушує права людини та характеризується відсутністю рівноваги між приватним життям і здоров'ям населення.

Наприклад, 13 квітня 2020 р. було прийнято Закон України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» з метою запобігання поширенню коронавірусної хвороби (COVID-19)»». Відповідно до вищезазначеного закону протягом періоду карантину або обмежувальних заходів, пов'язаних із розповсюдженням коронавірусної хвороби (COVID-19), і протягом 30 днів із дати його скасування, персональні дані можуть оброблятися без згоди особи. Зокрема, це можуть бути дані про стан здоров'я, місце госпіталізації чи самоізоляції, прізвище, ім'я, по батькові, дату народження, місце проживання, роботи (навчання). Обробка даних без згоди проводиться з метою протидії поширенню коронавірусної хвороби (COVID-19), способом, зазначеним у рішенні про встановлення карантину, за умови, що такі дані використовуються виключно з метою протиепідемічних заходів. Протягом 30 днів після закінчення карантинного періоду такі дані знеособлюються та, якщо це неможливо, знищуються [6].

Тож формулювання нового закону неоднозначне. Визначення мети обробки персональних даних як протидії поширенню коронавірусної хвороби (COVID-19) і можливість їх використання виключно з метою здійснення протиепідемічних заходів – це дуже широке за своїм змістом поняття. Воно може довільно трактуватися органами державної влади, підприємствами, установами, організаціями, котрі надають медичну допомогу. Закон мав би містити більш конкретизоване визначення мети та кола суб'єктів, чиї персональні дані будуть оброблятися [15].

Слід зазначити, що ст. 8 Конвенції про захист прав людини й основоположних свобод передбачає, що кожен має право на повагу до приватного та сімейного життя, до свого житла і кореспонденції [7]. Водночас Конституція України зазначає, що жодна особа не може втручатися в її особисте та сімейне життя, крім випадків, передбачених Конституцією України. Важливо зазначити, що ст. 64 Конституції України встановлено, що конституційні права і свободи людини та громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України. За умов надзвичайного стану можуть встановлюватися окремі обмеження прав і свобод із зазначенням строку дії цих обмежень [8]. 25 березня 2020 р. Кабінет Міністрів прийняв рішення про введення надзвичайного стану на всій території України. Закон від 13 квітня 2020 р. встановлює підстави для такого втручання у зв'язку з боротьбою з розповсюдженням коронавірусної хвороби (COVID-19).

У преамбулі згаданого Закону України «Про захист населення від інфекційних хвороб» передбачено, що він визначає правові, організаційні та фінансові принципи діяльності державного та місцевого рівнів, підприємств, установ та організацій, спрямованих на запобігання розповсюдженню інфекційних хвороб, локалізацію та ліквідацію спалахів та епідемій, встановлює права, обов'язки та відповідальність юридичних і фізичних осіб у сфері захисту населення від інфекційних хвороб.

Отже, на підставі вищезазначених фактів можемо зазначити, що Закон України «Про захист персональних даних» регулює правовідносини, пов'язані з обробкою персональних даних, а Закон України «Про захист населення від інфекційних хвороб», на нашу думку, повинен регулювати лише права фізичних осіб у сфері захисту проти інфекційних хвороб. У цьому контексті виникає логічне питання: чому в Закон, який регулює захист персональних даних, не було внесено змін до обробки персональних даних, і взагалі, які юридичні підстави для обмеження такого конституційного права за надзвичайних ситуацій?

Відповідно до ст. 2 Закону України «Про захист персональних даних», персональні дані – це інформація або сукупність відомостей про фізичну особу, яку ідентифікують або можуть конкретно ідентифікувати [9]. Також у ст. 11 Закону України «Про інформацію», інформація про фізичну особу (персональні дані) – це інформація або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [10]. Таким чином, можна стверджувати, що обробка персональних даних дозволена виключно з метою протиепідемічних заходів.

Відповідно до ст. 1 Закону України «Про захист населення від інфекційних хвороб» протиепідемічні заходи – це сукупність організаційних, медичних, ветеринарних, інженерних, адміністративних та інших заходів, що вживаються для запобігання розповсюдженню інфекційних хвороб, локалізації та ліквідації їх осередків, спалахів та епідеміц [11]. Тому неможливо чітко визначити, хто має право обробляти згадані дані, оскільки чіткого переліку суб'єктів немає, та зазвичай це органи державної влади, підприємства, установи, організації, які надають медичну допомогу.

Якщо тлумачити правило буквально, такий перелік слід шукати в рішенні про встановлення карантину. Тож за необхідне вважаємо проаналізувати визначення поняття «карантин», закріплене у ст. 1 Закону України «Про захист населення від інфекційних хвороб», яка тлумачить, що такі заходи повинні нести лише адміністративний і медичний характер.

Привертає увагу процедура обробки даних, а саме збір, реєстрація, накопичення, зберігання, адаптація, модифікація, поновлення, використання та розповсюдження, знеособлення, знищення персональних даних. Незрозуміло, яка група осіб підлягатиме такій примусовій обробці даних (лише особи з COVID-19, контактні особи або хтось взагалі).

Якщо поглянути на Закон буквально, то виявляється, що рішення про карантин стосується кожної людини. Тому важливо визначити обсяг даних, що підлягають обробці. Цей перелік не є вичерпним, але визначено, що він включає такі дані, як: стан здоров'я; місце госпіталізації або самоізоляції; повне ім'я; дата народження; місце проживання; робота (навчання).

Хоча знову залишається незрозумілим, з якою метою вводяться такі обмеження щодо обробки персональних даних без згоди, якщо згода на обробку персональних даних не потрібна у випадках, коли така інформація необхідна для охорони здоров'я, медичної діагностики, догляду чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я за умови, що такі дані обробляє уповноважений суб'єкт (медичний працівник, фізична особа-підприємець, котрий отримав ліцензію в порядку, встановленому законодавством тощо), який відповідає за забезпечення захисту персональних даних і який керується законами та іншими нормативними актами про лікарську таємницю.

Тобто ухвалений 13 квітня 2020 р. Закон України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)» не виводить персональної інформації про хворих на коронавірус з-під захисту закону і не дозволяє лікарям та іншим посадо-

вим особам розголошувати цю інформацію, а журналістам – поширювати її в засобах масової інформації. Деякі журналісти вважають, що прізвища та інші персональні дані хворих є суспільно важливою інформацією, а отже, можуть вільно поширюватися, але таке твердження не відповідає дійсності. Водночас варто пам'ятати, що знеособлена інформація, яка не містить персональних даних і не дозволяє встановити особу хворого, може розміщуватися в засобах масової інформації і не порушує вимог законодавства [16].

У свою чергу, персональні дані пацієнтів у електронну систему охорони здоров'я можуть вводити визначені медзакладом уповноважені особи. Це може бути медичний працівник або інша уповноважена особа закладу охорони здоров'я, лікар-ФОП, який має ліцензію на провадження господарської діяльності з медичної практики, та його працівники. На них має поширюватися дія законодавства про лікарську таємницю, і вони повинні забезпечувати захист таких персональних даних. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом.

Звертаємо увагу на те, що персоналізовані дані (усі дані про пацієнта, які містяться у декларації, а із запровадженням електронного рецепта й електронної медичної картки – медична інформація і призначення) доступні тільки лікарю, з яким підписана декларація, та лікарю, до якого пацієнт приходить за направленням. Коли у системі з'являться медичні дані, пацієнт зможе сам вирішувати, кому він додатково надає доступ [17]. Тому ми вважаємо, що медичні працівники не повинні давати згоду на обробку персональних даних своїх пацієнтів, оскільки така обробка здійснюється відповідно до положень закону. В Україні така форма як «Інформована добровільна згода пацієнта на обробку персональних даних» була скасована, і передача персональних даних третій стороні не повинна повідомлятися власником, якщо передача здійснюється державою й органами місцевого самоврядування.

Пацієнт насамперед повинен знати, що доступ до його персональних даних (всієї інформації, яку містить декларація, електронна медична картка й електронний рецепт) має тільки лікар, з яким він підписав відповідну декларацію, а також лікар, до якого пацієнт звернеться за медичною допомогою за направленням. Інші фахівці зможуть отримати доступ до персональних даних пацієнта (коли вони з'являться в системі) тільки з його дозволу. Однак інформація про пацієнта доступна також і медичному працівнику, який вносить її в систему. Тому, щоб уникнути будь-якої витоку інформації про пацієнта, лікувальний заклад делегує для цієї роботи певних уповноважених співробітників. Їх обирають із числа медичних працівників або інших уповноважених осіб установи охорони здоров'я. При виборі осіб, котрі будуть вносити інформацію про пацієнта в електронну систему, слід керуватися такими принципами: на них має поширюватися законодавство про лікарську таємницю, вони повинні забезпечити захист персональних даних пацієнта У всіх випадках, крім передбачених законодавством, ці посадові особи зобов'язані попередити розголошення будь-якої персональної інформації, яка їм стала відома у зв'язку з виконанням ними посадових обов'язків у будь-який спосіб.

ЛІТЕРАТУРА

1. COVID-19 daily new cases South Korea 2020. URL: https://www.statista.com/statistics/1102777/south-korea-covid-19-daily-new-cases/ (дата звернення: 17.02.2021).
2. Південна Корея не перемогла коронавірус, а навчилася з ним жити без локдауну. *Бабель* : веб-сайт. URL: https://babel.ua/texts/56485-pivdenna-koreya-ne-peremogla-koronavirus-a-navchilasya-z-nim-zhiti-bez-lokdaunu-lyudey-masovo-testuyut-a-likari-detektivi-stezhat-za-kozhnim-infikovanim-po-gps-za-materialom-bloomberg (дата звернення: 17.02.2021).
3. Геращенко припускає контроль за дотриманням карантину через моніторинг мобільних мереж. *Радіо Свобода* : веб-сайт. URL: https://www.radiosvoboda.org/a/news-herashchenko-kontrol-za-karantynom-cherez-mobilni/30505782.html (дата звернення: 17.02.2021).
4. Уряд зобов'язав Мінцифри забезпечити функціонування електронного сервісу «дій вдома», зокрема, інформаційної системи епідеміологічного контролю за поширенням COVID-19, що є частиною сервісу. *УКРІНФОРМ* : веб-сайт. URL: https://www.ukrinform.ua/rubric-society/3011567-v-ukraini-zapuskaut-dodatok-dij-vdoma-dla-kontrolu-samoizolacii.html (дата звернення: 17.02.2021).
5. Мінцифра використовує big data для боротьби з пандемією. *Міністерство та Комітет цифрової трансформації України* : веб-сайт. URL: https://thedigital.gov.ua/news/mintsifra-vikoristovue-big-data-dlya-borotbi-z-pandemieyu (дата звернення: 17.02.2021).
6. Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19) : Закон України від 13 квітня 2020 р. № 555-IX. URL: https://zakon.rada.gov.ua/laws/show/555-20#text (дата звернення: 17.02.2021).
7. Конвенція про захист прав людини та основоположних свобод. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 17.02.2021).
8. Конституція України від 28 червня 1996 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 17.02.2021).
9. Про захист персональних даних: Закон України від 01 червня 2010 р. № 2297-VI. URL: https://kodeksy.com.ua/pro_zahist_personal_nih_danih/statja-2.htm (дата звернення: 17.02.2021).
10. Про інформацію: Закон України від 02 жовтня 1992 р. № 2657-XII**.** URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 17.02.2021).
11. Про захист населення від інфекційних хворобл: Закон України від 6 квітня 2000 р. № 1645-III**.** URL: https://zakon.rada.gov.ua/laws/show/1645-14#text(дата звернення: 17.02.2021).
12. Мобільний додаток «Дія». URL: https://play.google.com/store/apps/details?id=ua.gov.diia.app (дата звернення: 17.02.2021).
13. Додаток «Дія»: як працює головний цифровий сервіс України. *Телеканал ZIK* : веб-сайт URL: https://zik.ua/article/dodatok_diia_yak_pratsiuie_holovnyi_tsyfrovyi_servis_ukrainy_958536 (дата звернення: 17.02.2021).
14. Екс-міністр інфраструктури України Володимир Омелян. сторінка Facebook. *Facebook*: веб-сайт. URL: https://m.facebook.com/volodymyr.omelyan?refsrc=https%3a%2f%2fm.facebook.com%2fvolodymyr.omelyan&_rdr (дата звернення: 17.02.2021).
15. Новий коронавірусний закон: обробка персональних даних без згоди власника та інші зміни законодавства. *LIGA360*: веб-сайт. URL: https://biz.ligazakon.net/analitycs/194650_noviy-koronavrusniy-zakon-obrobka-personalnikh-danikh-bez-zgodi-vlasnika-ta-nsh-zmni-zakonodavstva (дата звернення: 17.02.2021).
16. Дозвіл на оброблення персональних даних хворих не дозволяє ЗМІ поширювати цю інформацію – юридичне роз'яснення. *Інститут масової інформації*: веб-сайт. URL: https://imi.org.ua/monitorings/dozvil-na-obrobku-personalnyh-danyh-hvoryh-ne-dozvolyaye-zmi-poshyryuvaty-tsyu-informatsiyu-i32661 (дата звернення: 17.02.2021).
17. Як медикам працювати з персональними даними пацієнтів. *Міністерство охорони здоров'я України*: веб-сайт. URL: https://moz.gov.ua/article/for-medical-staff/jak-medikam-pracjuvati-z-personalnimi-danimi-pacientiv (дата звернення: 17.02.2021).