УДК 343.3/.7:004.056 (477)

БАТИРГАРЕЄВА В.С., *доктор юридичних наук, професор,* головний науковий співробітник Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України", директор НДІ ВПЗ ім. академіка В.В. Сташиса НАПрН України.
ORCID: https://orcid.org/0000-0003-3879-2237.

КРИМІНОЛОГІЧНИЙ АНАЛІЗ ЗАГРОЗ ПРАВАМ І СВОБОДАМ ЛЮДИНИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ ПІД ЧАС КАРАНТИНУ У ЗВ'ЯЗКУ З ПАНДЕМІЄЮ CoVID-19

Анотація. *У статті здійснено кримінологічний аналіз основних загроз правам і свободам людини, на які вона може наразитися в інформаційному просторі під час запровадження й реалізації карантинних заходів у зв'язку із пандемією CoVID-19. До таких загроз віднесено поширення неправдивої інформації, стигматизацію певних суб'єктів – окремих осіб, соціальних груп, народів, країн та правопорушення, вчинення яких стає можливим завдяки кіберпростору.*

Ключові слова: *інформаційний простір, пандемія CoVID-19, дезінформація, інфодемія, стигматизація, правопорушення.*

Summary. *The article provides a criminological analysis of the main threats to human rights and freedoms that may be encountered in the information space during the introduction and implementation of quarantine measures in connection with the CoVID-19 pandemic. Such threats include the dissemination of false information, the stigmatization of certain actors (individuals, social groups, peoples, countries) and offenses, which are made possible by cyberspace.*

Keywords: *information space, CoVID-19 pandemic, misinformation, infodemia, stigmatization, offenses.*

Аннотация. *В статье осуществлен криминологический анализ основных угроз правам и свободам человека, с которыми может столкнуться человек в информационном пространстве при введении и реализации карантинных мер в связи с пандемией CoVID-19. К таким угрозам отнесены: распространение ложной информации, стигматизация определенных субъектов (отдельных лиц, социальных групп, народов, стран) и правонарушения, совершение которых становится возможным благодаря киберпространству.*

Ключевые слова: *информационное пространство, пандемия CoVID-19, дезинформация, инфодемия, стигматизация, правонарушения.*

Постановка проблеми. Інформаційний простір як головний комунікатор соціуму є неодмінною складовою всіх процесів його життєдіяльності. Намагаючись розширити межі та можливості цього простору, людство завжди рухалося у напрямку відшукання нових засобів комунікації, що згодом призвело до формування інформаційного суспільства, феномен якого сьогодні досить активно досліджується у філософії, глобалістиці, соціології, інформатиці, педагогіці, мистецтві і навіть у футурології. У 2011 році вільний доступ до мережі Інтернет визнано ООН як фундаментальне право людини [1]. Наслідком цього є небачене раніше збільшення впливу інформаційної складової на соціальне буття, якими б концептуальними характеристиками ми його не наділяли – постіндустріальне, інформаційне, ринкове, громадянське [2, с. 5].

Разом із тим невпинний розвиток інформаційних технологій, що спостерігається у світі принаймні в останні кілька десятків років, супроводжується необхідністю

© Батиргареєва В.С., 2021

розв'язання низки супутніх проблем, як-от: осмислення можливостей єдиної системи комунікативних зв'язків, заснованих на "цифрі", як нової моделі соціальної кооперації та прояву глобалізації сучасного соціуму як такої; прогнозування сценаріїв переходу останнього до якісно нової фази свого розвитку – інформаційної (постіндустріальної, постмодернової); аналіз негативних і позитивних наслідків, що випливають із цього факту, та розробка шляхів блокування несприятливих сценаріїв у процесі повсюдного впровадження цифрових технологій у ті чи інші сфери життя – економіку, політику, медицину, освіту, культуру тощо; кримінологічний моніторинг ситуації із правопорушеннями, вчинення яких зумовлюється можливостями саме цього простору; та ін. Не заперечуючи проти того факту, що цифровий розвиток є безумовним драйвером світового прогресу, слід пам'ятати, що цифровізація, активне зростання технологій та інноваційних досягнень незмінно породжують ризики та загрози [3], що мають стали предметом ретельного кримінологічного вивчення.

Таким чином, у суспільстві склалася парадоксальна ситуація: загальний тренд покращення якості комунікації стикається із загрозами, котрі є сателітами цього тренду. У подібній діалектиці, за словами відомого американського письменника та статистика Насіма Талеба, чимало "чорних птахів – лебедів". Це означає, що ми живемо під знаком непередбачуваності. І така непередбачуваність криється не лише у тому, що суспільство дедалі більше входить у суперечливу епоху цифрових трансформацій, а й у дії, припустимо, природних чинників, розвиток яких на певному етапі важко піддається поясненню й прогнозуванню. Одним із таких чинників є поширення донині невідомих хвороб.

Результати аналізу наукових публікацій. Щоб уявити, який обсяг публікацій сьогодні присвячується проблемі пандемії CoVID-19 у цілому та аналізованій тематиці, зокрема, достатньо зазначити, що сьогодні коронавірус став одним з основних інфоприводів [4], тому близько 88 % актуальних новин в соцмережах присвячені коронавірусу [5]. Така лавиноподібна ситуація спостерігається й у науці. З огляду на це дуже важко здійснити хоча б поверхневий аналіз підготовленої літератури. Тому уявляється правильним обмежитися посиленням лише на доробок тих українських авторів, які, на наш погляд, системно висвітлюють проблему небезпек інформаційного простору для пересічної людини, а також здійснюють соціально-правове та кримінологічне вивчення негативних соціально-правових та кримінологічних наслідків пандемії CoVID-19. До числа фахівців першої групи належать Д.С. Азаров, В.М. Брижко, В.Д. Гавловський, О.В. Голубєв, О.Г. Данильян, О.П. Дзьобань, М.В. Карчевський, В.А. Ліпкан, В.Г. Пилипчук, Н.А. Савінова, В.Ф. Фурашев, А.О. Ярошенко та ін. Що стосується науковців, увага яких спрямована на набуття знання щодо подолання чисельних негативних наслідків пандемії, які проявляються у різних соціальних сферах, то вважаємо за доцільне у цій статті згадати лише про науковий доробок творчого колективу фахівців НДІ ВПЗ, адже останніми за підтримки Національного фонду досліджень України виконується проєкт "Соціально-правові та кримінологічні наслідки поширення пандемій та шляхи їх усунення в Україні" (В.І. Борисов (керівник проєкту), В.С. Батиргареєва, Д.П. Євтєєва, А.В. Каліліна, М.Г. Колодяжний, С.С. Шрамко). Поміж іншого, зазначеними науковцями розглядається й проблема впливу інформаційного простору на поточну ситуацію із подолання аналізованої пандемії. Разом із тим серед різноманіття чисельних загроз слід виділити й ті загрози правам і свободам громадян, нейтралізація яких є невідкладною справою вже зараз.

Метою статті є, по-перше, виділення та кримінологічний аналіз породжених інформаційним простором найбільш помітних негативних явищ, що створюють ризики, у тому числі криміногенні, та призводять до порушення прав і свобод людини; по-друге, з'ясування впливу та розкриття зв'язку цих негативних явищ із ситуацією пандемії

CoVID-19 та реалізацією карантинних заходів; по-третє, експозиція деяких пропозицій щодо запобігання та зменшення негативного ефекту для прав і свобод людини від загроз інформаційного простору за часів пандемії.

Виклад основного матеріалу. Станом на 18 червня 2021 р. від CoVID-19 у світі померло 3 842 377 осіб, в Україні – 54 091 [6]. У подібній ситуації нескладно уявити, наскільки інформаційний простір є перевантаженим відомостями про світову коронакризу та ситуацію через цю кризу в окремих країнах, а також відомостями, що так чи інакше з нею пов'язані. Сама якість і націленість (іншими словами, вплив) усіх цих відомостей на певні сфери життєдіяльності, групи осіб та ін. стають великою проблемою так званої гігієни сучасного інформаційного простору, адже інформаційний простір з усіма його можливостями стає придатним інструментом для вчинення різноманітних протиправних діянь, "палітру" яких навіть неможливо до кінця уявити. У відповідності до щорічної доповіді Всесвітнього економічного форуму (21 – 24 січня 2020 р.) стосовно головних ризиків, з якими може зіштовхнутися світ, серед п'яти основних загроз було вказано на проблеми з кіберзлочинністю та у сфері охорони здоров'я [7]. Як показали подальші події 2020 р., ці загрози в умовах коронакризи дійсно стали відчутними, як ніколи.

Беручи до уваги висловлене, введений з метою протидії пандемії CoVID-19 режим карантинних заходів, з одного боку, істотно прискорив процеси діджіталізації суспільства і навіть виявився стимулом для пошуку і масового започаткування нових режимів роботи – дистанційного та змішаного, активного впровадження інструментів е-урядування, розвитку форм онлайн-навчання, телемедицини, Інтернет-торгівлі, проведення zoom-зустрічей та ін. А з другого боку, інформація про це лихо завдяки можливостям глобалізації поширюється у найкоротший строк. Таким чином, захист прав і свобод людини в інформаційному просторі має будуватися з урахуванням низки факторів, як-от: характеру та видів можливих загроз, поширеності останніх, професійних, вікових, будь-яких особистісних та ін. якостей особи і, безумовно, загальної ситуації, в якій перебуває світ. Від захищеності прав і свобод, а отже, й самої людини буде залежати стан безпеки людини в інформаційному просторі. У зв'язку з цим, ще раз повторимося, на характер і способи захисту прав людини в інформаційному просторі у теперішній час накладатиме відбиток ситуація пандемії, що викликала введення режиму карантинних заходів. Не вдаючись у сутність цих заходів, лише зазначимо, що найбільш істотних обмежень у світі та в Україні зазнали насамперед права громадян на свободу пересування, освіту та мирні зібрання. Тією чи іншою мірою обмежень зазнали і права людини у сфері культури, праці, зайняття підприємницькою діяльністю, навіть у сфері медицини.

Сьогодні навіть складно уявити таку сферу життєдіяльності суспільства, яка була б абсолютно захищена від ризиків інформаційного характеру. Проте, виходячи з буквального, або вузького, тлумачення інформаційного простору, взятого в аспекті функціонування мережі інформаційних комунікацій, слід відзначити, що трьома головними загрозами для людини, які здатний генерувати, поширювати та підживлювати інформаційний простір в умовах карантину, є фейки, правопорушення та стигматизація, умовою існування яких є рух відповідної інформації за допомогою засобів та інструментів цього простору.

Якщо перелічені небезпеки, на які може наразитися людина в інформаційному просторі під час здійснення карантинних заходів, представити у вигляді умовної піраміди, то у підґрунті цієї піраміди знаходяться випадки генерування й поширення неправдивої інформації (найчастіше йдеться про так звані фейки, або фейкові новини). Інформація подібного роду може зачіпати інтереси максимально невизначеного кола

споживачів, а тому порушення права на отримання правдивої інформації носитиме масовий характер. Слід визнати, що рух фейків не обмежують ані державні кордони, ані соціально-економічні та політичні формули буття, ані релігійні системи. У свою чергу, середину такої піраміди складають випадки стигматизації певних суб'єктів. При цьому обсяги прояву стигматизації інколи виявляються вражаючими, оскільки піддаватися стигмі можуть цілі народи, країни, континенти. Нарешті, на вершині "карантинної" піраміди небезпек знаходяться правопорушення, за якими завжди стоять конкретні особи. Звісно ж, стигматизація та поширення неправдивої інформації так само можуть набувати ознак протиправних діянь, однак ці масові феномени, як правило, є не персоніфікованими, на відміну від протиправної поведінки, яка, повторимося, завжди є проявом "злої волі" конкретної особи.

Отже, першим блоком небезпек, здатних порушити права і свободи в інформаційному сегменті буття і тим самим створити стан небезпеки для людини, є недостовірна інформація, поширення якої сьогодні називають не інакше, ніж "мережева чума" [8].

В абз. 5 п. 15 постанови Пленуму Верховного Суду України (нині – Верховний Суд) "Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи" від 27.02.09 р. № 1 зазначається, що *недостовірною вважається інформація*, яка не відповідає дійсності або викладена неправдиво, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені) [9].

Поряд із поняттям недостовірної інформації так само використовуються поняття дезінформування, дезінформації та фейків, або фейкових новин. Так, у ДСТУ 3396.2-97 "Захист інформації. Технічний захист інформації. Терміни та визначення" від 01.01.98 р. у п. 7.5 дається *визначення дезінформування*, під яким розуміється спосіб технічного захисту інформації, який полягає у формуванні свідомо хибної інформації для унеможливлення несанкціонованого доступу до істинної інформації [10]. Що стосується інформаційних фейків (новин), то існує чимало їх визначень. Однак, уявляється, головне не в різноманітті визначень та пошуку універсального поняття, а в тому, якій сфері суспільних відносин подібна інформація може завдати шкоди.

На нашу думку, у кримінологічному сенсі під недостовірною інформацією, поширеною *в умовах запровадження карантинних заходів* під час епідемій та пандемій слід розуміти навмисне спотворення суспільно значимої інформації стосовно географії й темпів поширення хвороби, її клінічних проявів і наслідків, способів і методів лікування, вживаних державою та суспільством засобів убезпечення та інших питань, пов'язаних із подоланням хвороби та її наслідків, а так само вигадування інформації, що подається під виглядом достовірних відомостей і що може загрожувати інтересам національної безпеки в сфері публічного здоров'я. Подібна інформація дезорієнтує суспільство, змушує вдаватися до хибних кроків, сприяє виникненню масових панічних настроїв і безладу, ескалації соціальної напруги, підриває віру людини у власні сили та ін. Крім того, фейкові новини паразитують на страхах, стресі і нездорової цікавості людини, припустимо, до теорій глобальних змов, центральними темами яких є "відсів" зайвої людської маси, що не потрапила до "золотого мільярду", біологічні війни, коронакриза як аналог третьої світової війни, "революція" роботів і т. п.

Щоб розробити кримінологічну систему заходів нейтралізації негативного впливу недостовірної інформація на громадян під час запровадження у країні карантинних заходів, а відповідно й загальний рівень криміногенності у суспільстві, слід зупинитися на джерелах, з яких люди черпають відповідну інформацію. За результатами

зазначеного вище дослідження під назвою “Соціально-правові та кримінологічні наслідки пандемій та шляхи їх усунення в Україні”, з’ясовано, що найчастіше інформацію, припустимо, про поширення пандемії в Україні та за кордоном респонденти отримують по телебаченню, радіо, із друкованої преси (63,9 % від усіх опитаних). Ще 46,2 % респондентів користуються офіціальними каналами Всесвітньої організації охорони здоров’я (далі – ВООЗ), МОЗ України в соціальних мережах та месенджерах; 34,2 % звертаються до інформаційних порталів новин в Інтернеті. Офіційними сайтами МОЗ і Національної служби здоров’я України користуються 32,2 % респондентів. Для 21,6 % осіб головним джерелом інформації є знайомі, друзі, колеги. На інші джерела інформації вказали 1,93 % (офіційні сайти РНБО України, університету Дж. Хопкінса й інших установ; безпосередньо в медичних закладах, де працюють респонденти, або зі службових документів та ін.)[*] .

Частка перевірених інформаційних джерел є не такою вже й значною. А тому вирішення проблеми пандемії CoVID-19 поєднується із необхідністю адекватної рефлексії на будь-які випадки недостовірної інформації, фреймом для яких стає глобалізація сучасного соціуму. Такий тандем недостовірної інформації та пандемії, який отримав назву інфодемії, окрім іншого, відтепер має братися до уваги у розробці будь-якого сценарію розвитку економічних, політичних та кримінальних реалій як національного, так і планетарного масштабів. Зазначені явища у своїй сукупності виявилися свого роду невідомими змінними глобального характеру, що впливають, у тому числі, й на визначення вектору прогнозних розрахунків майбутнього кількісно-якісного стану злочинності (принаймні на найближчу перспективу) та розробку кримінологічних стратегій запобігання їй. Недаремно Генеральний директор ВООЗ Т.А. Гебрейэсус зазначив: “Ми не просто боремося з епідемією, ми боремося з інфодемією” [11].

У цьому плані цікаво навести досвід деяких країн.

Якщо звернутися до досвіду Китаю, то в цій країні з початку березня 2020 р. поширення дезінформації у соціальних мережах визнається кримінальним правопорушенням. Аналогічний закон існує в Індонезії та Саудівській Аравії. Встановлена кримінальна відповідальність за поширення “коронавірусної” дезінформації й у деяких країнах пострадянського простору – в Узбекистані, Молдові, РФ [12, с. 4].

Унаслідок відсутності у чинному законодавстві України відповідальності за систематичне умисне поширення недостовірної інформації (дезінформації, фейків) наразі й у нашій країні назріла така потреба.

Останніми роками у світі поширюється феномен соціальної стигматизації осіб, що захворіли на певні хвороби. Причому стигматизуються цілі соціальні групи, народи країн, що може призводити до актів дискримінації. Це зумовлюється виникненням нових вогнищ небезпечних хвороб та стрімкістю й масштабами їх розповсюдження на певних територіях. Коли хвороби вважаються смертельними, люди, які наражаються на великий ризик інфікування, подають свої страхи, звинувачуючи у нових спалахів хвороб когось або якусь групу людей [13]. За визначенням ВООЗ, *соціальна стигматизація в питаннях здоров’я* – це виникнення негативної асоціації певного захворювання з певною особою або групою осіб із спільними характеристиками, що під час спалаху захворювання може відбиватися у розповсюдженні упередженості, стереотипів, дискримінації та сегрегації щодо таких людей і/або в утраті ними свого статусу внаслідок передбачуваного у них зв’язку з хворобою [14]. Тому й невипадково, що

[*] *Прим. авт*. Сумарно кількість наданих відповідей перевищує 100 %, що пояснюється тим, що респонденти могли одночасно користуватися кількома джерелами інформації.

проблема соціальної стигматизації осіб, що захворіли на ті чи інші види психічних і фізичних недугів, є не лише предметом обговорення серед фахівців у галузі охорони здоров'я та інших наук про суспільство і людину, а й викликає необхідність ведення гострої соціальної полеміки у форматі "must know".

Фахівці роблять цікаве спостереження про те, що у наш час з'являється тривожна лексика, що нагадує про концтабір (іспанською): permiso para conducir ("перепустка"), permiso para circular ("дозвіл на пересування"), guetto ("гетто"), aislamiento ("ізоляція"), а так само виникають постапокаліптичні одиниці: nueva normalidad ("нова нормальність"), postpandemia ("постпандемія") [15, с. 1383]. Тому невипадково зазначається, що тема CoVID-19 знаходить нові грані як дослідницька проблема світового масштабу в соціокомунікативному і лінгвістичному аспектах [15, с. 1369]. ВООЗ наводить приклади бажаних і небажаних слів і словосполучень (виразів). Наприклад, стверджується, що бажано називати хворих "людьми з CoVID-19", "особами, які лікуються від CoVID-19", "одужують від CoVID-19" або "померли після зараження CoVID-19". У свою чергу, небажано називати хворих та людей, які можливо інфікувалися, "хворими на CoVID-19" або "жертвами коронавіруса", "підозрілими" або "підозрюваними на CoVID-19 пацієнтами". І зовсім неприпустимо говорити, що люди "поширюють CoVID-19", "заражають оточуючих" або "розносять вірус", оскільки під цим мається на увазі вина цих людей у навмисній передачі інфекції [14].

Що стосується сумного українського досвіду поширення стигматизації, то початок актів стигматизації мав місце наприкінці лютого 2020 р. у Нових Санжарах Полтавської області у вигляді протестів, причиною яких стало рішення Уряду розмістити у місцевому шпиталі Національної гвардії людей, евакуйованих із китайського міста Ухань, в якому на той час знаходився епіцентр хвороби [16]. Однак пройде небагато часу, і ця хвороба стане сприйматися як щось буденне, коли знаходження поряд з явно хворою людиною перестане викликати негативну реакцію із приводу недотримання останньою карантинних заходів. До речі, об'єктом стигматизації і дискримінації ставали й конкретні люди, які заразилися хворобою або стосовно яких є інформація, що вони можуть виявлятися безсимптомними носіями інфекції [17, с. 2716]. Сьогодні побічно свідчити про деяку стигматизацію осіб, які хворіли на CoVID-19, може й той факт, що 36,7 % українських громадян намагаються обмежувати контакти з такими особами. Разом із тим в Україні стигматизація осіб, хворих на коронавірусну хворобу, не досягає критичних масштабів, щоб поставало завдання вживання будь-яких невідкладних заходів. Однак із метою превенції вже сьогодні слід вживати відповідних заходів у правовій, інформаційній та морально-культурологічній площинах, що, по суті, є кримінологічним загальносоціальним запобіганням.

Нарешті, ще одним видом небезпеки, на яку може наразитися людина в інформаційному просторі під час здійснення карантинних заходів, є кримінально карані правопорушення. На думку фахівців, актуальність проблематики інформаційної безпеки зумовлена синергетичним ефектом, що головним чином визначається двома факторами, а саме: сплеском великої уваги до проблеми на рівні ЗМІ, що призвело до різкого зростання комп'ютерних вторгнень, заснованих на методах соціальної інженерії; карантинними заходами, які реалізують сучасні можливості віддаленої роботи, що змінило усталені режими безпечного і сталого функціонування систем в Інтернеті [5]. На додаток до цього, як правильно зазначається А.В. Калініною, у межах боротьби із загрозою для життя та здоров'я населення, якою є коронавірусна хвороба, влада багатьох держав запровадила жорсткі карантинні заходи, а отже, змінила звичний уклад життя соціальних груп [18, с. 40].

Під час запровадження карантинних заходів перебування людини в кіберпросторі призводить до збільшення ймовірності стати жертвою від низки правопорушень, фоном для яких стають саме умови соціальної ізоляції. На додаток до вже відомих загроз у кіберпросторі людина наражається на ризики, інформаційним лейтмотивом яких стає пандемія і все, що з нею пов'язано. Таким чином, загальним для цих злочинів моментом, що дозволяє виокремити та проаналізувати їх, є обстановка і засоби вчинення. Так, кіберзлочини вчиняються в обстановці реалізації карантинних заходів, що передбачають і соціальну ізоляцію, і присутність у буденному житті людини відповідних суб'єктів (лікарів, фармацевтів, працівників різних соціальних служб та ін.), "імітація" діяльності яких може ставати джерелом небезпеки для пересічного громадянина, і збільшення часу, проведеного людиною в кіберпросторі, який, власне, й стає основною загрозою правам і свободам людини, та ін. Крім того, засновуючись на положеннях розділу XVI Особливої частини КК України, можна визначити, що засобом вчинення кіберзлочинів є електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі і мережі електрозв'язку, тобто інформаційно-комунікаційні технології.

За свідченням Д.В. Дубова, ще у середині десятих років XXI ст. в Україні в повному обсязі були присутні всі ключові "класичні" кіберзлочини (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків тощо), кількість яких зростає щороку [19, с. 210]. Сьогодні в умовах реалізації карантинних заходів проблема кіберзлочинності лише загострилася. Експерти в галузі комунікаційно-інформаційних технологій виділяють три причини збільшення кількості кіберзлочинів. По-перше, саме карантин створив умови для хакерів-початківців, які з появою вільного часу активно "експериментують"; по-друге, злочинці використовують масову стурбованість людей темою захворювання на коронавірус, вдаючись до фішингу і так званої соціальної інженерії; по-третє, масовий перехід працівників на нові умови роботи в період карантину з віддаленим доступом до робочих комп'ютерних систем робить уразливою інформацію, яка створюється і передається інформаційно-комунікаційними засобами [20]. При цьому якихось принципово нових видів загроз не з'явилося, оскільки злочинцями використовуються ті самі методи доступу до "цікавої" інформації, як і раніше (інтернет-фішинг, СМС-фішинг, вішинг, скімінг, шимінг, шкідливі програми, спам, соціальна інженерія та ін.) або вчиняються інші протиправні діяння відповідної спрямованості (піратство у галузі інтелектуальної власності в Інтернеті, протиправний контент, мальваре, рефайлінг [21], голосові повідомлення, встановлення застосунків, спрямованих на стеження за людиною, та ін.). Єдине, що додалося нового, так це перенесення зловмисниками акцентів на те, в який спосіб "ефективніше" робити втручання, беручи до уваги перехід робітників на дистанційний режим роботи з використанням особистих комп'ютерних приладів. Наприклад, зафіксовані випадки, коли працівнику приходила розсилка нібито від служби IT-підтримки або відділу кадрів його компанії з інформацією про звільнення у зв'язку з необхідністю оптимізації штату у складних пандемічних умовах, і більш докладну інформацію про відповідне рішення пропонувалося дізнатися із прикріпленого до листа зараженого файлу або при переході за посиланням на сайт, який краде персональні дані (звісно ж, про загрози таких листів або посилань адресат не здогадувався). За такою схемою "працюють" й повідомлення, що надійшли нібито від страхової компанії із приводу закінчення терміну дії договору медичного страхування, податкових органів, благодійних некомерційних організацій, авіакомпаній, торговельних компаній щодо "суперпропозицій" і "суперакцій" тощо. У результаті збитків зазнавали як самі працівники, персональні дані яких потрапляли

третім особам, так і компанії, які наражалися на локальні і мережеві зараження [3]. За інформацією глави Національної поліції України, у 2020 р. у країні було зареєстровано понад 5 тис. кіберзлочинів, за вчинення яких вдалося оперативно затримати 106 осіб [22].

На наш погляд, масив кіберзлочинів у період реалізації карантинних заходів можна поділити на протиправні діяння, у "сценарії" вчинення яких ключовою є тема коронавірусу, та "традиційні" злочини, вчинення яких безпосередньо не зумовлюється коронавірусною тематикою, хоча їх кількість (у бік збільшення) корелює із загальною ситуацією у суспільстві. Це збільшення пояснюється, зокрема, тим, що до тих злочинців, які вже займалися Інтернет-шахрайством (фальшиві Інтернет-магазини, Інтернет-аукціони, "корисні" сайти різноманітних послуг, телекомунікаційні засоби зв'язку тощо), приєдналися нові віртуальні злочинці, які до періоду карантинних заходів займалися злочинною діяльністю в реальності, адже кіберпростір привернув увагу багатьох зловмисників тим, що в ньому злочинний дохід може виявлятися не меншим, ніж в реальному просторі, але при більш низькому рівні ризиків.

До першої групи нами віднесено продаж нелегального медичного обладнання і медичних препаратів за допомогою відповідних торговельних Інтернет-платформ; шахрайство з приводу придбання та продажу медичних засобів індивідуального захисту (захисних масок, масок-респіраторів, антисептичних засобів, ліків і т. п.), продуктів харчування, речей індивідуального вжитку, розповсюдження "високоефективних" ліків від коронавірусу або препаратів, які унеможливлюють зараження ним, пропозиції щодо дезінфекції приміщень, автомобілів, речей і т. п. від коронавірусу так само через мережу Інтернет [18, с. 41]; кібершахрайство, яке "засновується" на експлуатації відповідної тематики (наприклад, пропозиції надати грошову допомогу у зв'язку із поширенням CoVID-19 від держави, органів місцевого самоврядування, посадовців, банківських установ, приватного сектора та ін. [18, с. 41], здійснити перехід за посиланням на певні сайти, що нібито містять корисну інформацію про хворобу, або скачати додаток для ознайомлення з актуальною інформацією про епідеміологічний стан) і фактично є лише приводом для отримання доступу до кредитно-фінансової та іншої важливої для людини інформації з метою подальшого її використання; кібератаки на медичні установи та інші об'єкти критичної інфраструктури, діяльність яких пов'язана із протидією пандемії, тощо. Тому можна говорити про новий різновид кіберзлочинців (найчастіше шахраїв) – "пандемічних" кіберзлочинців. Так, ще у квітні 2020 р. повідомлялося, що кіберполіція з початку пандемії викрила низку підпільних ділків та вилучила понад тисячі несертифікованих тестів коронавірусу, понад 2,5 тисяч літрів підроблених антисептичних засобів, а також майже 35 тис. медичних масок та респіраторів [20]. До того ж, за даними ВООЗ, щодня створюється близько 2 тис. сайтів про коронавірус, чимало з яких, вочевидь, можуть бути вірусними (наприклад, зловмисники викрадають облікові дані, логіни та паролі за допомогою "карт поширення коронавірусу") [20].

Аналізуючи першу групу кіберзлочинів, кілька слів необхідно сказати про виклики та загрози у сфері охорони здоров'я. Сьогодні, на жаль, медичні установи, компанії розробників вакцин та гуманітарні організації входять до переліку об'єктів критичної інфраструктури, що найчастіше атакуються кіберзлочинцями. Причому йдеться не лише про "традиційні" фішингові атаки з метою розкрадання відомостей про персонал і пацієнтів, що знаходяться на лікуванні або самоізоляції, для подальшого продажу цих даних, а й про "експлуатацію" самої приналежності закладів з охорони здоров'я до тих установ, до яких пересічні громадяни апріорі мають довіру. Так, зловмисниками нібито від імені таких установ масово розсилаються бюлетені, новини, дайджести з інформацією

про ситуацію із поширенням хвороби в певному регіоні та заходи боротьби з нею. Насправді ж подібні відправлення є ні чим іншим, як листом з фішинговим посиланням чи вірусною програмою. Після того, як особа відкриє цей лист або перейде за посиланням, "сценарій" стає традиційним. Відносно новим об'єктом кібератак у частині можливого використання персональних даних у теперішній час є система телемедицини, що популярна на Заході під час домашнього лікування. До того ж останнім часом навіть ВООЗ стає об'єктом дедалі більшої кількості кібератак та кіберінцидентів. Наприклад, хакери намагалися викрасти логіни та паролі її співробітників, запустивши фішинговий сайт, що імітував внутрішню систему електронної пошти організації [20].

Інколи злочинці з корисливою метою вдаються до кібератак на інформаційні системи медичних закладів за допомогою комп'ютерного вірусу, що унеможливлює роботу всіх електронних ресурсів, в яких міститься, наприклад, інформація з медичних карт пацієнтів, призначення лікарських препаратів, проведення процедур тощо. І зовсім цинічними в умовах пандемії видаються випадки блокування злочинцями інформаційних систем медичних установ, що відповідають за коректну й безперебійну роботу високотехнологічного медичного обладнання – техніки, що підтримує життєдіяльність людського організму, забезпечує роботу томографів, апаратів штучної вентиляції легень, операційної апаратури тощо (так званий Інтернет речей). Це робиться зловмисниками так само з метою отримання коштів за розблокування програм, відповідальних за коректну роботу медичного обладнання. За свідченням О.С. Маркова, що засновується на частоті згадувань у мережі Інтернету про розглядувану проблему, сьогодні кібератаки на медичні заклади складають 4 % від усіх загроз у кіберпросторі, релевантних коронавірусу [5]. Отже, серед прав людини, що порушуються у такий своєрідний спосіб, насамперед йдеться про її право на життя та здоров'я, котрі у період розповсюдження коронавірусної інфекції стають, напевно, найістотнішими правами.

Що стосується групи "традиційних" злочинів, вчинення яких безпосередньо не корелює з коронавірусною тематикою, то в їх "бутті" спостерігаються свої закономірності, що існували ще до пандемії та будуть існувати й після її завершення.

Висновки.

Дослідження проблеми особливостей захисту прав, свобод і безпеки людини в інформаційному просторі в умовах карантинних заходів дозволяє зробити кілька висновків принципового характеру.

По-перше, трьома істотними видами загроз чисельним благам людини в інформаційному просторі під час пандемії CoVID-19 є: заповнення цього простору неправдивою інформацією, що набуває характеру інфодемії, множення випадків стигматизації певних суб'єктів та вчинення кримінально караних правопорушень. Тому кримінологічний аналіз саме цих видів загроз має покладатися у підґрунтя розробки напрямів протидії небезпечним викликам інформаційного простору.

По-друге, проблематика кримінологічних важелів інформаційного убезпечення прав і свобод людини стає надзвичайно актуальною в період запровадження режиму карантинних заходів. У ситуації надзвичайної активності зловмисників єдине, що залишається, – змінити загальну парадигму протидії кіберзагрозам із наступальної на оборонну, в якій пріоритет віддаватиметься саме захисту інформації та запобіганню можливим загрозам. А враховуючи те, що "світ вже не буде таким як раніше", слід максимально сконцентруватися на тому досвіді, який людство отримало в пандемічний період, поширивши його мейнстрими й на часи "постпандемії".

По-третє, якщо є надія, що сила впливу інфодемії та проявів стигматизації рано чи пізно ослабне, тощо стосується злочинних проявів, то це негативне явище, на жаль, "резистентне" до зміни векторів актуальності тих чи інших суспільних проблем.

Напевно, можна стверджувати, шо "виник" новий феномен – пандемічний злочинець, протиправна поведінка якого знаходить свій прояв насамперед в інформаційному просторі. Всі злочини пандемічного періоду доцільно поділити на ті, сутність вчинення яких зумовлена темою коронавірусу, та "традиційні" злочини, вчинення яких розвивається за власним "сценарієм", хоча загальна їх кількість й корелює із режимом карантину. При цьому особливу тривогу викликають кібератаки на об'єкти критичної інфраструктури, від коректної роботи яких залежить безпека громадян. Саме протидія таким проявам має стати стратегічним напрямом запобіжної діяльності під час реалізації у країні карантинних заходів.

Використана література

1. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. United Nations. A/HRC/17/27. URL: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_ en.pdf (дата звернення: 25.06.2021).

2. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти. Харків: Майдан, 2011. 244 с.

3. Ключевская Н. Информационная безопасность и CoVID-19: рекомендации для бизнеса и граждан. URL: https://www.garant.ru/article/1421147 (дата звернення: 28.06.2021).

4. Отт М. "Хіт-парад" вірусних новин. Як медіа писали про CoVID-19? https://voxukraine.org/virusni-novini (дата звернення: 30.06.2021).

5. Марков А. Информационная безопасность в условиях пандемии CoVID-19. URL:https://expert.ru/2020/04/9/informatsionnaya-bezopasnost-v-usloviyah-pandemii-CoVID-19 (дата звернення: 25.06.2021).

6. Коронавирус в мире: данные по странам и регионам. URL: https://www.bbc.com/russian/news-51706538 (дата звернення: 20.06.2021).

7. The Global Risks Report 2020. *World Economic Forum*. 15th Edition. Geneva: Marsh & McLennan and Zurich Insurance Group, 2020. 102 p.

8. Sherry Ricchiardi. Фактчекинг распространяется повсеместно благодаря этим ресурсам. https://ijnet.org/ru/story/фактчекинг-распространяется-повсеместно-благодаря-этим-ресурсам (дата звернення: 30.06.2021).

9. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи: Постанова Пленуму Верховного Суду України від 27.02.09 р. № 1. URL: https://zakon.rada.gov.ua/laws/show/v_001700-09 (дата звернення: 25.06.2021).

10. Захист інформації. Технічний захист інформації. Терміни та визначення: ДСТУ 3396.2-97 від 01.01.98 р. URL: https://tzi.com.ua/478.html (дата звернення: 18.06.2021).

11. Дорошенко К. Світові інтелектуали про наслідки пандемії коронавірусу для людства. URL: https://suspilne.media/20654-svitovi-intelektuali-pro-naslidki-pandemii-koronavirusu-dla-ludstva (дата звернення: 25.06.2021).

12. Коваленко М., Беленькая М., Тарасенко П. Вакцина от фейков. Как мир борется с дезинформацией о пандемии. *Коммерсантъ.* 2020. № 57. С. 4. – (31 марта).

13. Michael McCauley, Sara Minsky, Kasisomayajula Viswanath. The H1N1 pandemic: media frames, stigmatization and coping. *BMC Public Health.* 2013. 13:1116. URL: http://www.biomedcentral.com/1471-2458/13/1116 (дата звернення: 22.06.2021).

14. Социальная стигматизация и CoVID-19 Руководство по предупреждению и преодолению стигматизации. URL: https://www.euro.who.int/__data/assets/ pdf_file/0007/432268/SocialStigmaAssociatedCoVID-19-rus.pdf (дата звернення: 29.06.2021).

15. Мустайоки А., Зорихина-Нильссон Н., Гусман Тирадо Р., Тоус-Ровироса А., Дергачева Д., Вепрева И., Ицкович Т. CoVID-19: катастрофа в языковом измерении разных стран. *Quaestio Rossica.* Vol. 8. 2020. No 4. P. 1369-1390.

16. Протесты в Новых Санжарах. URL: https://ru.wikipedia.org/wiki/Протесты_в_Новых_Санжарах (дата звернення: 30.06.2021).

17. Vladyslava S. Batyrgareieva, Oleh A. Zaiarnyi, Sabriie S. Shramko. Prevention of the stigmatization of individuals in response to digital tracking (concidering CoVID-19 issue). *Wiadomości Lekarskie*. 2020. Tom LXXIII nr 12 cz. II. P. 2715-2721.

18. Калініна А.В. Пандемія вірусу VS правопорядок: кримінологічний прогноз. *Питання боротьби зі злочинністю:* зб. наук. пр. / редкол.: Б.М. Головкін та ін. Харків: Право, 2020. Вип. 39. С. 39-45.

19. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.

20. Стрій Є. Don’t click shit! Як вберегтися від кіберзлочинців у час пандемії. URL: https://investigator.org.ua/ua/publication/224967 (дата звернення: 25.06.2021).

21. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606 (дата звернення: 28.06.2021).

22. У 2020 році Нацполіція викрила більше ніж 5000 кіберзлочинів. URL: https://www.kmu.gov.ua/news/u-2020-mu-nacpoliciya-vikrila-ponad-5-000-kiberzlochiniv (дата звернення: 16.06.2021).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~