УДК 343.9:004.738.5:616-036.21

С. С. Шрамко,
канд. юрид. наук, в.о. вченого секретаря НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України

А. В. Калініна,
канд. юрид. наук, науковий співробітник відділу кримінологічних досліджень НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України

КРИМІНАЛЬНО-ПРАВОВІ ТА КРИМІНОЛОГІЧНІ ЗАГРОЗИ В ІНТЕРНЕТ-ПРОСТОРІ У ПЕРІОД ПАНДЕМІЇ[1]

У статті надається загальна характеристика кримінально-правових та кримінологічних загроз в Інтернет-просторі, що набули особливого розповсюдження або виникли у період пандемії в Україні та світі. Визначено ризики, пов'язані із діджиталізацією сфери охорони здоров'я в Україні і за кордоном. Зазначено, що Інтерполом на міжнародному рівні було виділено три найпоширеніших види кібератак, від яких постраждали фізичні та юридичні особи протягом пандемії: 1) функціонування шкідливих доменів; 2) розповсюдження шкідливого програмного забезпечення; 3) завантаження програм-вимагачів.

Проаналізовано прояви фішингу та інших видів кібершахрайств, пов'язаних із COVID-19. Підкреслено, що сприйняття фейкової інформації (залежно від її характеру), може спричиняти поширення серед населення панічних настроїв, формуванню агресії стосовно певних груп осіб тощо.

Визначено, що протягом пандемії COVID-19 наслідком збільшення кількості «екранного часу» як серед дорослих, так і серед дітей, сприяло активізації дій, спрямованих на сексуальне розбещення дітей в Інтернеті, кіберзалякування, підштовхування до ризикованої поведінки в мережі, поширенню потенційно небезпечного контенту.

Наведено, що за оцінками експертів реалізація кримінально-правових та кримінологічних загроз в Інтернет-просторі у 2020 р. завдала збитків у розмірі понад 1 % світового ВВП.

Ключові слова: *загрози в Інтернет-просторі, кіберзлочинність, фішинг,фейк, діджиталізація медицини.*

[1] Статтю підготовлено на виконання проєкту «Соціально-правові та кримінологічні наслідки поширення пандемій та шляхи їх усунення в Україні» (реєстр. номер 2020.01/0155), що виконується за підтримки Національного фонду досліджень України.

Постановка проблеми. Збентеження населення глобальною проблемою – потенційним зараженням вірусом SARS-CoV-2 (коронавірусом) та наслідками хвороби, яку він викликає, – більш, ніж благодатний ґрунт для різного роду маніпуляцій із людською свідомістю. Адже емоція страху – головна зброя в цьому випадку. До неї додаються ще і стресовий стан, в якому опинилася особа через введення карантинних заходів в Україні різного ступеня суворості, острах за життя і здоров'я (як своє, так і близьких і рідних), недовіра до статистичних даних про кількість хворих і померлих саме від коронавірусної хвороби та різноманітних видів штамів коронавірусу, збентеження щодо якості, доступності та побічних наслідків вакцинації від цієї хвороби, сюжети у ЗМІ з відповідної тематики (нерідко негативного забарвлення) тощо. Отже, людина готова повірити у будь-що, аби убезпечити себе від реальної чи потенційної загрози, що одразу ж намагаються використати зловмисники, у тому числі й ті, які «працюють» в Інтернет-просторі. Адже злочинність завжди чутлива до змін у суспільстві. Особливо, коли ці зміни – потенційне середовище для її продукування.

Життя сучасної людини важко уявити без Інтернету. Наразі для багатьох саме цей ресурс є першочерговим в отриманні інформації. Тому із появою нового фактора (загроза захворювання на коронавірус та вакцинація від нього), який значно вплинув на життєдіяльність людини (у виді масштабних карантинних заходів, що запроваджувалися у державі в різний час), Інтернет-простір став дещо по-новому використовуватися і злочинцями.

Аналіз останніх досліджень і публікацій. Дослідження питання убезпечення населення в Інтернет-просторі та винайдення ефективних засобів запобігання кіберзлочинності постійно знаходиться у фокусі підвищеної уваги науковців і практиків. Зокрема, різні аспекти зазначеної проблематики розглядувалися у працях таких вітчизняних учених, як: Д. С. Азаров (D. S. Azarov), В. С. Батиргареєва (V. S. Batyrgareieva), П. Д. Біленчук (P. D. Bilenchuk), М. В. Карчевський (M. V. Karchevs'kyj),

М. О. Кравцова (M. O. Kravtsova), А. А. Музика (A. A. Muzyka), В. Г. Пилипчук (V. H. Pylypchuk), О.Е. Радутний (O.E. Radutnyj), Н. А. Савінова (N. A. Savinova). Значних здобутків у дослідженні цього питання досягли зарубіжні дослідники, зокрема: T. J. Holt, A. Bossler, J. Hawdon, E.R. Leukfeldt та ін. Загалом слід відзначити, що пандемічний стан, у якому опинився світ, розширив горизонти наукового і практичного інтересу щодо загроз в Інтернет-просторі.

Метою статті є надання загальної характеристики найбільш поширеним кримінологічним загрозам в Інтернет-просторі, що виникли не лише стосовно громадян, а й для установ різної форми власності, об'єктів критичної інфраструктури та ін., протягом пандемії COVID-19 в Україні та світі.

Виклад основного матеріалу.

Пандемія змінила звичайний спосіб життя більшості населення планети, а разом із тим зробила людей і суспільство надзвичайно уразливими майже в усіх аспектах життєдіяльності. Під час цієї кризи люди більше, ніж будь-коли, стали покладатися на комп'ютерні системи, мобільні пристрої та Інтернет для віддаленої роботи, навчання, спілкування, здійснення покупок, обміну та отримання інформації, пом'якшення впливу соціального дистанціювання тощо. Збільшення кількості користувачів Інтернету, і часу, проведеного в мережі, у поєднанні з почуттям розгубленості, тривоги і страху, стали сприятливим середовищем для кримінальної протиправності у кіберпросторі. Стресовий стан через карантинні обмеження та щоразу нову інформацію про коронавірус і вакцинацію проти нього лише підсилив ймовірність виникнення емоції страху та панічних настроїв серед населення. За перших симптом ГРВІ або застуди людина, замість звернення до лікаря (навіть дистанційного), з більшою ймовірністю починає шукати інформацію в Інтернет-просторі. Такий підхід сприяє виникненню трьох головних загроз:

1) погіршення стану здоров'я особи (наслідки самолікування можуть бути катастрофічні);

2) підвищення ризику стати жертвою неправомірних діянь, для вчинення яких використовується Інтернет-простір пов'язаних із COVID-19;

3) негативний вплив на авторитет держави.

Поринання у віртуальний світ пов'язане із низкою загроз, що мають яскраво виражене кримінальне забарвлення або ж кримінологічний характер. За повідомленням кіберполіції протягом 2020 р. від громадян України було отримано понад 41,5 тис звернень з приводу неправомірних дій в Інтернеті[2]. Необхідно зазначити, що протидія кіберзлочинам та іншим правопорушенням, що вчиняються в Інтернеті, була визначена пріоритетом у діяльності Департаменту кіберполіції у 2020 році[3]. Значення боротьби із вказаними правопорушеннями підкреслюється тим, що від кібератак страждають не лише приватні особи, але й об'єкти критичної інфраструктури, компанії, підприємства, організації та установи, державні органи і органи місцевого самоврядування, у тому числі й лікарні, та ін.

Зокрема, зарубіжні дослідники (Williams C., Chaturvedi R., Chakravarthy K.) повідомляють, що з початком поширення пандемії COVID-19 лікарні, медичні центри й інші установи охорони здоров'я потерпають від масованих кібератак, що здійснюються із метою отримання викупу за викрадену з їх баз даних інформацію. Захист персональних даних пацієнтів набуває особливої актуальності у світлі того, що наразі галузь охорони здоров'я знаходиться в процесі серйозної еволюції: більшість медичних карт пацієнтів переведені в онлайн-формат, лікарі також ведуть консультації та прийоми пацієнтів онлайн, а лікарні, відповідно, формують бази даних про них. Однак по мірі того, як триває адаптація до епохи цифрових технологій,

[2] У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайства в Інтернеті. URL: https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/.

[3] Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf. С. 8.

виникає низка проблем, пов'язаних із загрозою конфіденційності, безпеки і кібербезпеки. Доступ до медичних карток пацієнтів – «золота жила» для кіберзлочинців, оскільки вони містять відомості і про дату народження, і про страховку у медичному закладі, і про генетичні дані, дані про стан здоров'я тощо, тобто таку інформацію, яку нелегко змінити на відміну від банківських карт або рахунків. Деякі фахівці зазначають, що така інформація є особливо привабливою для хакерів, тому що прибуток від її продажу може бути у 10-20 разів більше[4].

Захист персональних даних осіб, якими володіють заклади охорони здоров'я, набуває значення і для України. Адже впровадження інформаційних технологій у сфері охорони здоров'я є одним із аспектів діджиталізації суспільних відносин в Україні. Головна мета такої діджиталізації створення ідеальної моделі дієвого сервісу із обслуговування громадян у сфері охорони здоров'я, у тому числі й полегшення надання медичних послуг лікарями. Отже, процес діджиталізації вітчизняної медицини є двостороннім: автоматизація прийняття рішень лікарями та доступ до послуги з охорони здоров'я пацієнтом. У літературі з метою розвитку електронної системи здоров'я пропонується створення медичних консультативно-діагностичних систем, або систем підтримки прийняття лікарських рішень, та введення електронних медичних карт[5]. Це сприятиме формуванню електронної охорони здоров'я (E-health), що передбачає використання інформаційно-комунікаційних технологій для поліпшення рівня охорони здоров'я, включаючи спосіб мислення та організації процесів у системі охорони здоров'я та пов'язаних сферах (науці, освіті, дослідницькій діяльності)[6]. E-health є галуззю, яка включає в себе не лише інформаційно-телекомунікаційні системи, але й такі компоненти, як органи управління,

[4] Williams C. M, Chaturvedi R, Chakravarthy K. Cybersecurity Risks in a Pandemic. J Med Internet Res. 2020; 22(9):e23692. DOI: 10.2196/23692. URL: https://www.jmir.org/2020/9/e23692/.

[5] Радзішевська Є. Б., Висоцька О. В. Інформаційні технології в медицині. E-health / за ред. В. Г. Кнігавка. Харків: ХНМУ, 2019. С. 57.

[6] Там само. С. 57.

нормативно-правова база, стандарти і контроль відповідності, кадрові ресурси, інфраструктура, стратегія та модель залучення інвестицій[7]. Головне, що функціонуватиме така система за допомогою такого ресурсу, як Інтернет.

Однак в реаліях нашого часу окреслені вище перспективи є, скоріше, надметою. Фактично держава робить лише перші кроки у цьому напрямі. Матеріально-технічне забезпечення багатьох медичних закладів є низьким, професіоналів, обізнаних на достатньому рівні навіть із основами роботи ПК, бракує. Рівень розвитку та забезпечення медицини у місті та селі разюче відрізняється. Окрім цього, не всі громадяни мають як доступ до інформаційно-технічних благ, так і відповідні навички користування ними.

Що ж до основної маси населення, то головним «порадником» та медичною консультативно-дорадчою системою є, як це не абсурдно визнавати, пошукові системи в Інтернеті. Адже головний елемент діджиталізації суспільних відносин перебуває у більшої частини громадян просто в руках – у смартфоні. Такий підхід має низку негативних, у першу чергу для самої особи та стану її здоров'я, наслідків. Значна кількість громадян просто не звертається до спеціалістів через те, що знаходить «правильну» інформацію про симптоми свого реального або уявного захворювання на інформаційних сайтах, у соціальних мережах і навіть у месенджерах. Особливо небезпечний характер такий Інтернет-серфінг набув у період пандемії COVID-19, що охопила значну кількість держав, набувши статусу світової.

Зважаючи на охоплення кібератаками фактично майже всього світу, Інтерполом на міжнародному рівні було виділено три найпоширеніших види кібератак, від яких постраждали фізичні та юридичні особи протягом пандемії:

[7] Радзішевська Є. Б., Висоцька О. В. Інформаційні технології в медицині. E-health / за ред. В. Г. Кнігавка. Харків: ХНМУ, 2019. С. 57.

1) функціонування шкідливих доменів. Одразу після початку пандемії в Інтернет-просторі було зареєстровано значну кількість доменів, що містять терміни: «coronavirus», «corona-virus», «covid19» тощо. І хоча деякі з них є не шкідливими веб-сайтами, кіберзлочинці щодня створюють тисячі нових сайтів для проведення спам-кампаній, фішингу або поширення шкідливих програм[8];

2) розповсюдження шкідливого програмного забезпечення. Шкідливі програми, шпигунське програмне забезпечення, комп'ютерні віруси і трояни – це перелік лише найбільш поширених загроз, які чекають на користувачів Інтернету, будучи вбудованими в інтерактивні карти і веб-сайти з інформацією про коронавірус. Ризик постраждати від перелічених програм може підстерігати користувачів і під час переходу за інтернет-посиланнями та у спам-повідомленнях, що завантажують шкідливе програмне забезпечення на комп'ютери або мобільні пристрої[9]. Кінцева мета правопорушників у такому випадку – отримання доступу до фінансової (платіжної) інформації користувача[10];

3) завантаження програм-вимагачів. Цей вид загроз в Інтернет-просторі здійснюється правопорушниками головним чином шляхом фішингу – шахрайських схем, що примушують людей розкривати персональну інформацію, таку як паролі або номери банківських або кредитних карт через підроблені веб-сайти або електронні листи. Про приблизні масштаби цієї проблеми можна скласти уявлення, ознайомившись із даними, зібраними компанією «Google» і проаналізовані компанією «Atlas VPN» (постачальником послуг віртуальної приватної мережі (VPN)). Так, відповідно до звіту, в січні 2020 р. «Google» зареєстрував 149 тис. активних

[8] Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception. URL: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats.

[9] Там само.

[10] Коронабизнес: как на пандемии коронавируса зарабатывают мошенники. URL: https://comments.ua/news/it/Internet/649763-koronabiznes-kak-na-pandemii-koronavirusa-zarabatyvayut-kibermoshenniki.html.

фішингових сайтів. У лютому того ж року це число майже подвоїлося і збільшилося до 293 тисяч. Однак у березні 2020 р. ця цифра становила 522 тис. – тобто зросла на 350% порівняно із січнем[11].

Необхідно зазначити, що фішинг – лише один із видів кібершахрайств. Проаналізуємо детальніше прояви фішингу та інших видів кібершахрайств, пов'язаних із COVID-19, нижче.

Фішинг. Загальнопоширеним як у науці, так і на практиці уявленням про фішинг є розуміння його як діяльності злочинців, що здійснюється шляхом поширення «гачків» для користувачів Інтернету: статистичних даних (переважно неправдивих) про COVID-19, інформації про методи, засоби та способи лікування коронавірусної хвороби, її профілактику та вакцинацію, різних видів компенсацій грошових коштів у зв'язку із карантином чи перенесенням захворювання (наприклад: державна допомога, благодійна допомога, відтермінування виплат за кредитами; компенсація за білети на різного виду транспорту, рейси якого відмінилися і т.п.), участь в інтернет-опитуваннях і т.п. Основна «зброя» фішингу – листи на електронну пошту, веб-сайти та додатки для смартфонів. Мета фішингу – отримання персональних банківських даних особи задля доступу до коштів жертви[12]. У технології фішингу можуть використовуватися назви міжнародних організацій, державних органів та установ (наприклад, Всесвітньої організації охорони здоров'я, Міністерства охорони здоров'я тощо). У сфері охорони здоров'я головним шахрайським «гачком» можна визнати продаж інформації про профілактику, лікування та вакцинацію від коронавірусної хвороби.

Одним із наймасштабніших проявів фішингу є широко обговорюваний у соцмережах злам влітку 2020 року такої соціальної мережі, як «Twitter». Зловмисником було взято під контроль облікові записи кількох

[11] Cyber-crime during the COVID-19 Pandemic. URL: http://f3magazine.unicri.it/?p=2085.

[12] Маніпуляції та шахраї під час епідемії коронавірусу: хто і як виграє, коли інші страждають. URL: https://rubryka.com/article/koronovirus-manipulation-crooks/.

знаменитостей у «Twitter» і шляхом шахрайських дій змушено людей відправити біткойни на певний обліковий запис. Внаслідок цих дій постраждали облікові записи та репутація компанії «Apple», Білла Гейтса, Каньє Уеста, Ілона Маска та ін. відомих осіб, а загальна сума збитків була оцінена майже в 117 тис. доларів. Талановитим зловмисником став 17-річний хакер із штату Флорид (США). Історія для нього закінчилася арештом[13].

Продаж засобів індивідуального захисту та антисептиків, що не відповідають медичним стандартам, тестів на наявність коронавірусу, медичних препаратів від SARS-CoV-2 та засобів його профілактики, інших продовольчих товарів та товарів особистого вжитку, що полягає у створенні фейкових сайтів, сторінок у соціальних мережах, каналів у месенджерах (Viber, Telegeam та ін.) і т.п. із пропозицією продажу такої продукції[14;15;16]. Наприклад, кіберполіція України за березень-квітень 2020 р. виявила та заблокувала діяльність 179 Інтернет-посилань, за якими шахраї ошукували громадян, продаючи неіснуючий товар, під час пандемії та встановила 236 осіб, що займалися вказаною вище діяльністю. Головна умова придбання таких товарів – стовідсоткова передплата їх вартості[17].

Окрім зазначеного, можна ще додати про **надшвидке поширення фейкової інформації** про коронавірус та його лікування, у тому числі, й від імені офіційних установ. За результатами проведеного фахівцями Науково-дослідного інституту вивчення проблем злочинності ім. акад. В. В. Сташиса НАПрН України опитування громадян щодо наслідків пандемії COVID-19 та шляхів їх усунення в Україні виявлено, що саме інформаційний простір є

[13] Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic. URL: https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html.

[14] Маніпуляції та шахраї під час епідемії коронавірусу: хто і як виграє, коли інші страждають. URL: https://rubryka.com/article/koronovirus-manipulation-crooks/.

[15] COVID-19: Increasing Risk of Cyber Fraud. URL: https://www.mccannfitzgerald.com/knowledge/disputes/covid-19-increasing-risk-of-cyber-fraud.

[16] З початку карантину кіберполіцейські перевірили 576 інформацій щодо можливих протиправних дій, пов'язаних з коронавірусом. URL: https://cyberpolice.gov.ua/news/z-pochatku-karantynu-kiberpoliczejski-pereviryly--informaczij-shhodo-mozhlyvyx-protypravnyx-dij-povyazanyx-z-koronovirusom-6129/.

[17] Там само.

основним каналом для отримання ними відомостей, що стосуються здоров'я. При цьому встановлено, що 63,9 % опитаних інформацію про стан поширення пандемії COVID-19 в Україні та за кордоном дізнавалися через ЗМІ (новини на радіо та телебаченні), 32,2 % – на офіційному сайті МОЗ України, 34,2 % – з інформаційних порталів новин, 21,6 % – від знайомих і друзів, а 1,9 % – з інших джерел[18]. Інформаційна «чистота» перелічених каналів, звичайно, не є ідеальною. Тому роз'яснення серед населення з приводу інформаційної гігієни у цьому та інших питаннях є одним із першочергових завдань, оскільки сприйняття фейкової інформації (залежно від її характеру), може спричиняти поширення серед населення панічних настроїв, формуванню агресії стосовно певних груп осіб (зокрема, за ознакою перенесення коронавірусної хвороби чи прояву окремих її симптомів, приналежністю до певних професій та ін.).

Домінування у дозвіллі «екранного часу» як серед дітей, так і серед дорослих має своїм наслідком ще низку, окрім перелічених вище, загроз для їх прав і свобод. Такими загрозами є:

1) *сексуальне розбещення дітей в Інтернеті*. Досить поширеним явищем є демонстрація сексуальної прихильності до малолітніх/неповнолітніх осіб у популярних соціальних мережах. Або іншими словами харасмент (від англ. «*harassment*» – переслідування, домагання). Така поведінка може виражатися у відвертих словесних домаганнях, відправленні матеріалів сексуального характеру та зворотному заклику поділитися власними фото і відео сексуального змісту[19];

2) *кіберзалякування (кібербулінг)*, що полягає у будь-якій агресивній, загрозливій діяльності, що здійснюється за допомогою електронних засобів зв'язку (електронна пошта, повідомлення в соціальних мережах тощо). За

[18] Звіт про результати анкетування щодо наслідків пандемії COVID-19 та шляхів їх усунення. Харків : Наук.-досл. ін-т вивч. пробл. злоч. ім. акад. В. В. Сташиса НАПрН України, 2021. 93 с. URL: https://ivpz.kh.ua/wp-content/uploads/2021/06/Звіт_анкетування-дороблений.pdf. С. 15.

[19] Bark's Annual Report on Children and Technology. URL: https://www.bark.us/annualreport.

даними застосунку Bark майже 72,8 % малолітніх та 78,4 підлітків ставали жертвою або свідком кіберзалякування в Інтернеті. Лише 11 % зізнаються про це батькам[20]. Діти вкрай уразливі та залежні від характеру коментарів щодо їх публікацій або фото, повідомлень, які вони отримують від своїх однолітків та інших незнайомців. За висловлення власних думок чи прихильності вони можуть бути виключені з соціальних груп, що ще більше посилює стрес і почуття ізоляції. Зазначене врешті-решт призводить до зворотної реакції, коли жертва перетворюється в ката;

3) *ризикована поведінка в мережі*. Фізичне дистанціювання і відсутність особистого спілкування під час локдауну, ізоліції чи самоізоляції призводять до різних «винаходів», які в інші часи і не спали би на думку. Одним із таких прикладів є секстинг (відправлення повідомлень відверто сексуального характеру) і обмін фото і відео в оголеному виді, оприлюднення чи передача третім особам таких зображень, які можуть використовуватися проти із метою булінгу, шантажу тощо;

4) *потенційно небезпечний контент*. Контент неприйнятного/шкідливого змісту є однією з найбільш поширених онлайн-загроз і для дітей, і для дорослих. Це, наприклад: підбурювання до самогубства і членоушкодження; матеріали, пов’язані з насильством або ксенофобією; ненависткські заклики до представників ЛГБТ; маркетинг, не призначений для дітей; дезінформація про COVID-19. За даними згадуваного застосунку Bark, 75,5 % малолітніх и 84,6 % підлітків вступали у розмови про алкоголь та наркотики; 35,1 % малолітніх і 54,4 % підлітків були залучені до членоушкодження або суїциду; 86,8 % малолітніх і 89,6 % підлітків говорили на насильницькі теми[21].

Оцінку збитків від кіберзлочинної діяльності протягом 2020 р. спробували зробити зарубіжні дослідники. Так, за даними американської

[20] Bark’s Annual Report on Children and Technology. URL: https://www.bark.us/annualreport.
[21] Там само.

компанії «McAfee», яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS) хакерські атаки протягом 2020 р. коштували світовій економіці понад трильйон доларів або 820 мільярдів євро. Цей збиток є на 50 % вищим, ніж був ще два роки тому, у 2018 р., встановили дослідники. Таким чином збитки, завдані хакерами у 2020 р., становлять понад 1 % світового ВВП, інформує агенція AFP[22]. Результати вказаного дослідження базуються на оцінці даних близько 1 500 ІТ-фахівців, які є співробітниками компаній, державних установ та різних організацій зі Сполучених Штатів Америки, Канади, Великобританії, Франції, Німеччини, Японії та Австралії. Для оцінювання збитків враховувалися не лише втрати цифрової власності, але й втрати робочого часу, протягом якого не працювали робочі системи, а також іміджеві втрати компаній і установ, які ставали об'єктами атак зловмисників. Автори дослідження вказують, що є й інші, приховані, втрати від кіберзлочинності, наприклад, зниження рівня задоволеності працівників своєю роботою[23].

Висновки. Пандемія COVID-19 – фактор, що вже тривалий час не зменшує рівня свого впливу на життя світової спільноти, одним із наслідків якого є значне зростання використання Інтернет-простору як в особистому, так і в корпоративному житті, виробничому процесі, навчанні тощо. Підвищення популяризації цього ресурсу сприяло активізації протиправної діяльності і виникненню через це низки загроз кримінально-правового та кримінологічного характеру. За оцінками експертів реалізація таких загроз в Інтернет-просторі у 2020 р. завдала збитків у розмірі понад 1 % світового ВВП. Міжнародний рівень цієї проблеми сприяв активізації міждержавного співробітництва у сфері боротьби із кіберзлочинністю та супутніми їй явищами, що, в першу чергу, виявилося в інформаційному обміні (наприклад, звітах, рекомендаціях і т.п. Інтерполу та ін.).

[22] Сидоржевський М. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження. URL: https://p.dw.com/p/3mN9i.

[23] Там само.

Список використаних джерел

1. У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайства в Інтернеті. URL: https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/.

2. Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf.

3. Williams C. M, Chaturvedi R, Chakravarthy K. Cybersecurity Risks in a Pandemic. J Med Internet Res. 2020; 22(9):e23692. DOI: 10.2196/23692. URL: https://www.jmir.org/2020/9/e23692/.

4. Радзішевська Є. Б., Висоцька О. В. Інформаційні технології в медицині. E-health / за ред. В. Г. Кнігавка. Харків : ХНМУ, 2019. 72 с.

5. Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception. URL: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats.

6. Коронабизнес: как на пандемии коронавируса зарабатывают мошенники. URL: https://comments.ua/news/it/Internet/649763-koronabiznes-kak-na-pandemii-koronavirusa-zarabatyvayut-kibermoshenniki.html.

7. Cyber-crime during the COVID-19 Pandemic. URL: http://f3magazine.unicri.it/?p=2085.

8. Маніпуляції та шахраї під час епідемії коронавірусу: хто і як виграє, коли інші страждають. URL: https://rubryka.com/article/koronovirus-manipulation-crooks/.

9. COVID-19: Increasing Risk of Cyber Fraud. URL: https://www.mccannfitzgerald.com/knowledge/disputes/covid-19-increasing-risk-of-cyber-fraud.

10. З початку карантину кіберполіцейські перевірили 576 інформацій щодо можливих протиправних дій, пов'язаних з коронавірусом. URL: https://cyberpolice.gov.ua/news/z-pochatku-karantynu-kiberpoliczejski-pereviryly--informaczij-shhodo-mozhlyvyx-protypravnyx-dij-povyazanyx-z-koronovirusom-6129/.

11. Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic. URL: https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html.

12. Звіт про результати анкетування щодо наслідків пандемії COVID-19 та шляхів їх усунення. Харків : Наук.-досл. ін-т вивч. пробл. злоч. ім. акад. В. В. Сташиса НАПрН України, 2021. 93 с. URL: https://ivpz.kh.ua/wp-content/uploads/2021/06/Звіт_анкетування-дороблений.pdf.

13. Bark's Annual Report on Children and Technology. URL: https://www.bark.us/annualreport.

14. Сидоржевський М. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження. URL: https://p.dw.com/p/3mN9i.

REFERENCES

1. U 2020 rotsi do kiberpolitsii nadiishlo ponad 30 tysiach zvernen shchodo shakhraistva v Interneti. URL: https://cyberpolice.gov.ua/news/u--roczi-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-shaxrajstva-v-interneti-8412/ [in Ukrainian].

2. Zvit Holovy Natsionalnoi politsii Ukrainy pro rezultaty roboty vidomstva u 2019 rotsi. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf [in Ukrainian].

3. Williams C. M, Chaturvedi R, Chakravarthy K. Cybersecurity Risks in a Pandemic. J Med Internet Res. 2020; 22(9):e23692. DOI: 10.2196/23692. URL: https://www.jmir.org/2020/9/e23692/.

4. Radzishevska, Ye. B., Vysotska, O. V. (2019). Informatsiini tekhnolohii v medytsyni. E health. Kharkiv: XNMU [in Ukrainian].

5. Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception. URL: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats.

6. Koronabiznes: kak na pandemii koronavirusa zarabatyvayut moshenniki. URL: https://comments.ua/news/it/Internet/649763-koronabiznes-kak-na-pandemii- koronavirusa-zarabatyvayut-kibermoshenniki.html [in Ukrainian].

7. Cyber-crime during the COVID-19 Pandemic. URL: http://f3magazine.unicri.it/?p=2085.

8. Manipuliatsii ta shakhrai pid chas epidemii koronavirusu: khto i yak vyhraie, koly inshi strazhdaiut. URL: https://rubryka.com/article/koronovirus-manipulation-crooks/ [in Ukrainian].

9. COVID-19: Increasing Risk of Cyber Fraud. URL: https://www.mccannfitzgerald.com/knowledge/disputes/covid-19-increasing-risk-of-cyber-fraud.

10. Z pochatku karantynu kiberpolitseiski pereviryly 576 informatsii shchodo mozhlyvykh protypravnykh dii, pov'iazanykh z koronavirusom. URL: https://cyberpolice.gov.ua/news/z-pochatku-karantynu-kiberpoliczejski-pereviryly--informaczij-shhodo-mozhlyvyx-protypravnyx-dij-povyazanyx-z-koronovirusom-6129/ [in Ukrainian].

11. Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic. URL: https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html.

12. Zvit pro rezultaty anketuvannia shchodo naslidkiv pandemii COVID-19 ta shliakhiv yikh usunennia. (2021). Kharkiv: Nauk.-dosl. in-t vyvch. probl. zloch. im. akad. V. V. Stashysa NAPrN Ukrainy. URL: https://ivpz.kh.ua/wp-content/uploads/2021/06/Звіт_анкетування-дороблений.pdf [in Ukrainian].

13. Bark's Annual Report on Children and Technology. URL: https://www.bark.us/annualreport.

14. Sydorzhevskyi, M. (2020). Kiberzlochyntsi u 2020 rotsi zavdaly u sviti zbytkiv na trylion dolariv – doslidzhennia. URL: https://p.dw.com/p/3mN9i [in Ukrainian].

Шрамко С. С., Калинина А. В. Уголовно-правовые и криминологические угрозы в Интернет-пространстве в период пандемии

В статье дается общая характеристика уголовно-правовых и криминологических угроз в Интернет-пространстве, которые приобрели особое распространение или возникли в период пандемии в Украине и мире. Определены риски, связанные с диджитализацией здравоохранения в Украине и за рубежом. Отмечено, что Интерполом на международном уровне было выделено три самых распространенных вида кибератак, от которых пострадали физические и юридические лица в течение пандемии: 1) функционирование вредных доменов; 2) распространение вредоносного программного обеспечения; 3) загрузка программ-вымогателей.

Проанализированы проявления фишинга и других видов кибермошенничества, связанных с COVID-19. Подчеркнуто, что восприятие фейковой информации (в зависимости от ее характера), может вызвать распространение среди населения панических настроений, формирование агрессии по отношению к определенным группам лиц и т.п.

Определено, что в течение пандемии COVID-19 в следствии увеличения количества «экранного времени» как среди взрослых, так и среди детей, способствовало активизации действий, направленных на: сексуальное развращение детей в Интернете, кибербуллинг, подталкивание к рискованному поведению в сети, распространению потенциально опасного контента.

Указано, что по оценкам экспертов реализация уголовно-правовых и криминологических угроз в Интернет-пространстве в 2020 г. нанесла ущерб в размере более 1% мирового ВВП.

Ключевые слова: *угрозы в Интернет-пространстве, киберпреступность, фишинг, фейк, диджитализация медицины*.

Shramko Sabriie, Kalinina Alina. Criminal law and criminological threats in the Internet during a pandemic

A general description of criminal law and criminological threats on the Internet, which have become particularly common or arose during the pandemic in

Ukraine and the world have been analyzed in the scientific paper. It is noted that during this pandemic people began to rely more than ever on computer systems, mobile devices and the Internet for remote working, education, communication, shopping, sharing and receiving information, minimization the influence of the social distancing, etc. Increasing of the number of Internet users and the time spent them online, combined with the feelings of confusion, anxiety and fear has become an enabling environment for criminal activity in the cyber space.

The risks associated with the digitalization of health care in Ukraine and abroad have been identified. It is noted, that Interpol has identified three the most common types of cyberattacks at the international level, which affected individuals and legal entities during the pandemic: 1) the functioning of malicious domains; 2) distribution of malicious software; 3) download extortion programs.

Phishing and other types of cyber fraud, related to COVID-19, were analyzed. It is emphasized, that the perception of fake information (depending on its content) can lead to the panic spreading among the population, the formation of aggression against certain groups of people and so on.

It was determined, that during the COVID-19 pandemic, the increasing of the amount of "screen time" among both adults and children contributed to the intensification of actions aimed at sexual abuse of children on the Internet, cyberbullying, incitement to risky online behavior, distribution of potentially dangerous content.

It is stated, that according to experts opinion, the implementation of criminal law and criminological threats on the Internet in 2020 caused losses of more than 1% of world GDP.

Key words: *threats in the Internet, cybercrime, phishing, fake, digitalization of medicine.*