УДК 343.3/.7:004.056 (477)

В. С. Батиргареєва,
докт. юрид. наук, проф., директор Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса НАПрН України, головний науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права» НАПрН України

ОСНОВНІ ТЕНДЕНЦІЇ КІБЕРЗЛОЧИННОСТІ КАРАНТИННОГО ПЕРІОДУ ТА ПРОТИДІЯ ЇЙ[1]

Проаналізовано новітні тенденції кіберзлочинності під час запровадження й реалізації карантинних заходів у зв'язку з поширенням у світі пандемії COVID-19 та деякі наслідки цього виду злочинності. Наведено причини, що призвели до появи у кримінальному середовищі нового феномену– так званого пандемічного злочинця, протиправна поведінка якого знаходить свій проявів насамперед в інформаційному просторі. Наголошено на небезпеці кіберзлочинності для об'єктив критичної інфраструктури, серед яких особливий наголос робиться на установах охорони здоров'я. Розкрито концептуальну ідею протидії кіберзлочинності, зміст якої визначатиме й стратегічні напрями цієї протидії на сучасному етапі розвитку суспільства.

Ключові слова: *інформаційний простір, пандемія COVID-19, «пандемічний злочинець», кіберзлочинність, протидія.*

Постановка проблеми. Складовою всіх процесів життєдіяльності людини, про який би етап розвитку людської цивілізації не йшлося, є комунікація. Саме завдяки необхідності людей спілкуватися один з одним існує й розвивається інформаційний простір як своєрідний субстрат опосередкування й спрямовування у певному русі узгоджених дій. Сучасний світ уже неможливо уявити без інформаційних технологій, в основі яких лежить використання комп'ютерної техніки та новітніх засобів електронних комунікацій, можливості яких активно впроваджуються в різноманітні галузі

[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.

людської діяльності. Поява таких технічних засобів, як Інтернет і мобільні пристрої, що дозволяють знаходитися в постійній комунікації членам суспільства один з одним, стала першою сходинкою діджиталізації і відповідно передвісником глобальних модифікацій соціальних інститутів та вектору розвитку суспільства в цілому. Напевно, можна стверджувати, до на Землі залишилося останнє покоління, що народилося у доцифрову епоху. Водночас, намагаючись з'ясувати можливості фактично нової парадигми буття сучасної людини, заснованої на законах розвитку інформаційного простору, слід відстежувати й небезпечні тенденції кіберпростору з тим, щоб завчасно розпізнати та нейтралізувати їх. Одна із таких небезпечних тенденцій інформаційного простору, що згодом лише набирає обертів, представлена кіберзлочинністю, котра включає, зокрема, випадки вторгнення в комп'ютерні системи (хакерство), онлайн-шахрайство у багатьох його видах і формах, економічне шпигунство (крадіжку комерційної таємниці), вимагання та «відмивання» грошей завдяки можливостям Інтернету, так звану крадіжку цифрової ідентичності, поширення контенту порнографічного характеру та ін.

Сьогодні справедливо стверджуються, що кіберзлочинність розвивається та зростає у відповідь на пандемію COVID-19, що стала одним із серйозних випробувань для людства за період, що минув від часів закінченням Другої світової війни. Як слушно зауважує М. В. Романов, саме пандемія COVID-19 гостро поставила питання і цифровізації (оскільки значна частина життя трансформується в он-лайн форму), і кібербезпеки (оскільки тепер захисту вимагає значно більша кількість суспільних відносин), і приватності (оскільки багато запроваджених протиепідемічних заходів суттєво порушують право на приватність і суміжні з ним права).

Стан розробки проблеми. Ще до пандемічного періоду проблема визначення тенденцій кіберзлочинності, здійснення кількісно-якісного аналізу та запобігання їй визнавалася однією з мейнстримових тем для

кримінально-правового й кримінологічного осмислення. Чимало зарубіжних і вітчизняних науковців приділяли увагу зазначеній проблематиці. Неабияке значення мають наукові праці останніх років таких зарубіжних учених, як D. Halder & K. Jaishankar (2016), M. Bossler & Tamar Berenblum (2019), R. Brandom (2019), J. T. Carback (2018), A. Janofsky (2018), M. T. Whitty (2019), D. Buil-Gil at al. (2020)S. Monteith at al. (2021) та ін. Серед вітчизняних вчених слід виділити напрацювання М. В. Карчевського, М. О. Кравцової, Л. В. Лефтерова, В. А. Ліпкана, В. Г. Пилипчука, Н. А. Савінової, О. Е. Радутного, О. М. Литвинова, Є. С. Назимка, В. Ф. Примаченка та ін. Крім того, до аналізу проблем правопорушень в інформаційному просторі починаючи з 2020 р. активно долучилися й учасники творчого колективу НДІ ВПЗ імені академіка В. В. Сташиса НАПрН України, які за підтримки Національного фонду досліджень України виконують 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. Калініна, М. Г. Колодяжний, С. С. Шрамко). Разом із тим слід відмітити, що в умовах лавиноподібної ситуації прирощення наукового знання, що сьогодні спостерігається у науці «карантинного періоду», важко здійснити навіть поверхневий аналіз літератури, присвяченої сучасним кримінальним загрозам кіберпростору та їх подоланню. Тому зосередимося лише на новітніх тенденції кіберзлочинності та протидії їй, на які звернено увагу під час реалізації зазначеного вище проєкту.

Метою статті є, по-перше, виділення новітніх тенденцій кіберзлочинності карантинного періоду; по-друге, аналіз наслідків цього виду злочинності, по-третє, визначення концептуальної ідеї та стратегічних напрямів протидії їй.

Виклад основного матеріалу. Станом на 7 липня 2021 р. від COVID-19 хвороби у світі вже померло 4 013 052 осіб, в Україні – 52 537. При цьому

коронакриза як така та обмеження у нормальному ритмі життя, що її супроводжують, викликали ситуацію, в якій інформаційний простір з усіма його можливостями стає придатним інструментом для вчинення різноманітних протиправних діянь, «палітру» яких навіть неможливо до кінця уявити. Ще у березні 2020 р. Європол опублікував доповідь під назвою «Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis» («Пандемічний спекулянт: як злочинці експлуатують кризу COVID-19»), в якій стисло викладено позицію аналітиків Європолу щодо головних змін у кримінальній дійсності пандемічного періоду. Так, відмічається, що правопорушники швидко скористалися можливостями, які відкриває криза, адаптуючи до цього свою злочинну діяльність або вдаючись до вчинення нових злочинних дій. Чинниками, що впливають на відмічені зміни, зокрема, є: високий попит на певні товари, як-от: захисне спорядження та фармацевтична продукція; зниження мобільності і потоку людей до ЄС або транзитом через ЄС; залишення громадян дома та дистанційний характер роботи з використанням можливостей Інтернет-простору; непомітність деяких кримінальних дій та їх перенесення у домашні умови або на онлайн-пристрої внаслідок обмежень у суспільному житті; вразливість людей через підвищення тривоги і страху; скорочення поставок певних незаконних товарів до ЄС. Водночас, ураховуючи інформацію, надану державами-членами ЄС та власними експертами, Європол робить висновок про зростання кіберзлочинності, шахрайства, продажу контрафактної медичної та санітарно-гігієнічної продукції, засобів індивідуального захисту та формування нового, так званого карантинного типу організованої злочинності, коли групи правопорушників реалізують цілі схеми, видаючи себе за представників органів влади та медиків із метою вчинення шахрайства і крадіжок.

Згідно зі ст. 1 Закону України «Про захист населення від інфекційних хвороб» карантин представляє собою адміністративні та медико-санітарні

заходи, що застосовуються для запобігання поширенню особливо небезпечних інфекційних хвороб. У нашій країні з метою дотримання режиму карантину, питання про встановлення та відміну якого порушуються перед Кабінетом Міністрів України центральним органом виконавчої влади, що забезпечує формування державної політики у сфері охорони здоров'я за поданням головного державного санітарного лікаря України, прийнято низку нормативних актів. Не вдаючись у сутність запропонованих за цими нормативно-правовими документами карантинних заходів, лише зазначимо, що найбільш істотних обмежень в Україні зазнали насамперед права громадян на свободу пересування, освіту та мирні зібрання. В тій чи іншій мірі обмежень зазнали і права людини у сфері культури, праці, зайняття підприємницькою діяльністю, навіть у сфері медицини. Водночас навіть складно уявити таку сферу життєдіяльності суспільства, яка була б абсолютно захищена від ризиків інформаційного характеру.

Одна з головних загроз для людини, яку здатний генерувати, поширювати та підживлювати інформаційний простір в умовах карантину, поряд з фейками та стигматизацією, повторимося, є кіберзлочини. Умови соціальної ізоляції є поживним ґрунтом для їх вчинення, а загальним для них моментом є обстановка (реалізація карантинних заходів, що супроводжуються соціальною ізоляцією та збільшенням часу, протягом якого людина перебуває у кіберпросторі, присутністю у буденному житті лікарів, фармацевтів, працівників різних соціальних інституцій та ін., «імітація» діяльності яких може ставати джерелом серйозної небезпеки) і засоби вчинення (інформаційно-комунікаційні інструменти).

Найпомітнішою тенденцією цих злочинів є збільшення їх кількості. Фахівці компанії Varonis Systems, що спеціалізується на створенні мережевих технологій та систем зберігання даних, зазначили, що 2020 рік приніс кілька викликів, виділили кілька тенденцій, що загрожують безпеці інформаційного простору. Так, зокрема, вказано, що працівники, які працюють в режимі

remote mode, як і раніше будуть мішенню для кіберзлочинців. Як побічний ефект віддаленої роботи збільшиться кількість витоків інформації із так званні хмарових платформ. Крім того, проблемою залишаться недостатні навички у сфері кібербезпеки, а в результаті збільшення пропускної здатності пристроїв, підключених за допомогою технології 5G, Інтернет речей так само стане більш уразливим для кібератак. Існує кілька причин подібної ситуації. Серед таких слід назвати карантин, що створив відповідні умови для хакерів-початківців, в яких з'явився вільний час для активних «експериментів»; масову стурбованість людей темою захворювання на коронавірус, чим користуються злочинці, що вдаються до фішингу і так званої соціальної інженерії; масовий перехід працівників у період карантину на нові умови роботи, що передбачає віддалений доступ до робочих комп'ютерних систем та робить уразливою інформацію, яка створюється і передається інформаційно-комунікаційними засобами. Водночас відмітимо, що якихось принципово нових різновидів загроз у кіберпросторі не з'явилося. Хіба що стають більш «витонченими» прийоми роботи кіберзлочинців. Як і раніше, правопорушники з метою доступу до «цікавої» інформації вдаються до інтернет-фішингу, СМС-фішингу, шкідливих програм, спамів, методів соціальної інженерії та ін., голосових повідомлень, установки застосунків, спрямованих на стеження за людиною, та ін. Але ж новою можна вважати тенденцію, яка полягає в тому, що зловмисниками перенесено акцент на те, в який саме спосіб «ефективніше» втручатися в роботу інформаційно-комунікаційних приладів, беручи до уваги масовий перехід робітників на дистанційний режим роботи з використанням, як правило, особистих комп'ютерних приладів. Так, зафіксовані випадки розсилки електронних листів працівникам нібито від служби IT-підтримки або відділу кадрів їх компанії з інформацією про їх звільнення у зв'язку з необхідністю оптимізації штату внаслідок складних пандемічних умовах. Для того, щоб дізнатися більш докладно про рішення керівництва компанії, працівникам

пропонувалося перейти за посиланням на сайт, який краде персональні дані (звісно ж, про таку загрозу 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 й мережеві зараження.

Цікаві дані із приводу збитку, що завдається хакерами, наводять американські дослідники. Так, вони стверджують, що у 2020 р. ці збитки у світовому вимірі склали понад 1 % світового ВВП, що складає 1 трлн. доларів. У свою чергу, за інформацією глави Національної поліції України у цьому ж році у нашій країні зареєстровано понад 5 тис. кіберзлочинів, за вчинення яких затримано 106 осіб.

Ще одна тенденція кіберлочинності карантинного періоду полягає в тому, що весь масив цих злочинів так чи інакше корелює з пандемією. Тому цей масив можна поділити на правопорушення, у «сценарії» вчинення яких визначальною є коронавірусна тематика, та «традиційні», або «звичні», злочини, вчинення яких безпосередньо не зумовлюється цією подією, хоча кількість таких злочинів (звісно ж, у бік збільшення) корелює з особливими умовами пандемічного періоду. Уявляється, що таке збільшення має пояснення, адже до числа інтернет-шахраїв приєдналися нові віртуальні злочинці, які до карантинного періоду займалися злочинною діяльністю в режимі оф-лайн.

Найпомітнішими злочинами, що віднесені нами до першою групи, сьогодні є: продаж нелегального медичного обладнання і медичних препаратів за допомогою відповідних торговельних інтернет-платформ; шахрайство з приводу придбанням та продажу медичних засобів індивідуального захисту (захисних масок, масок-респіраторів, антисептичних

засобів, ліків тощо), 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; кібершахрайство, яке «засновується» на експлуатації відповідної тематики і фактично є лише приводом для отримання доступу до кредитно-фінансової та іншої важливої для людини інформації з метою подальшого її використання (наприклад, пропонується 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, отримати грошову допомогу у зв'язку із поширенням COVID-19 від держави, органів місцевого самоврядування, посадовців, банківських установ, приватного сектора та ін.); кібератаки на медичні установи та інші об'єкти критичної інфраструктури, діяльність яких пов'язана із протидією пандемії, тощо. Тому все частіше стверджується про «виникнення» нового різновиду кіберзлочинців (найчастіше шахраїв) – «пандемічних» кіберзлочинців, або шахраїв.

Тенденцією сьогодення є так само той факт, що кіберзлочини представляють серйозну загрозу для сфери охорони здоров'я, адже медичні установи, компанії розробників вакцин та гуманітарні організації та фонди входять до числа об'єктів критичної інфраструктури, що найчастіше атакуються кіберзлочинцями. Навіть ВООЗ стає об'єктом кібератак з метою активації фішингових програм. Причому йдеться не лише про «традиційний» фішинг із 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 і від імені яких нібито розсилаються бюлетені, новини, дайджести з інформацією про ситуацію із поширенням хвороби в певному регіоні та

заходи боротьби з нею. Насправді ж подібні відправлення представляються серйозну небезпеку для користувачів інформаційно-комунікаційних мереж.

Відносно новим об'єктом кібератак є 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. В умовах пандемії злочинці не гребують й блокуванням 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 званих 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.

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.

Перелічені тенденції у кіберзлочинності карантинного періоду ще більше загострили необхідність перегляду підходів та стратегій боротьби з кіберзлочинністю. Так, якщо раніше суспільство пов'язувало ефективність протидії саме з активною наступальною тактикою, спрямованою на унеможливлення кібератак зловмисників, то у теперішній час пріоритет належить саме захисту інформації від можливих загроз. Говорячи мовою експертів у сфері ІТ-технологій, необхідно переосмислити підхід до інформаційної безпеки та максимально скоротити «площу атак», а ті корисні

уроки із забезпечення інформаційної безпеки, що отримуються в період пандемії, використовувати і в постпандемічний період. Іншими словами, від наступальної позиції під гаслами викоренити кіберзлочинність у найкоротший час суспільство переходить до «оборонної» стратегії убезпечення інформації від кіберзлочинців та утрудненого доступу до неї, адже кіберзлочинність віднині стає «одвічною» проблемою, що завжди існуватиме поряд із процесами діджиталізації суспільства. Переорієнтація на такий підхід є особливо важливою для пересічних громадян, суб'єктів малого та середнього бізнесу, а так само для державних установ, які не здатні утримувати самостійні служби інформаційної безпеки, користуватися надійними каналами зв'язку, оновлювати достатньо часто свій технологічний парк тощо.

Тут кілька слів потрібно сказати про причини, що зумовлюють запровадження саме «оборонної» стратегії. Ці причини насамперед криються у сучасному форматі спілкування, характері виробничих процесів і ведення бізнесу. Отже, убезпечення інформації є своєрідною антитезою, по-перше, стиранню кордонів між корпоративними та особистими інформаційно-комунікаційними пристроями, що пояснюється тим, що фахівці багатьох організацій і корпорацій працюють вдома на власних комп'ютерах, ноутбуках, комунікаторах, ступінь захищеності яких є, як правило, нижчою за корпоративні інформаційні ресурси; по-друге, залежності інформаційної безпеки від людського фактору, що характеризується недостатнім рівнем знань про можливі загрози в інформаційному просторі, засоби й методи їх розпізнавання, а головне, про способи упередження та усунення наявних загроз в умовах цифровізації періоду «COVID-катастрофи»; по-третє, недостатньому фінансуванню забезпечення інформаційної безпеки або навіть скороченню витрат на це.

Чітко розуміючи основні причини вразливості суб'єктів інформаційного простору, можна визначити ключові особливості

кіберзахисту останніх в умовах карантинних заходів. І найпершим напрямом в оборонній стратегії, спрямованої проти кіберзлочинів, слід назвати інформаційну просвіту та ознайомлення із тематикою, яку найчастіше експлуатують зловмисники у періоди епідемій, пандемій та інших природних і соціальних катаклізмів, та конкретними заходами інформаційної безпеки на відповідних рівнях – «елементарному» побутовому (елементарні інформаційні кампанії) та професійному (за допомогою проведення спеціального інструктажу, семінарів, тренінгів, курсів тощо). Якщо йдеться про діяльність організаційно структурованих суб'єктів управління, бізнесу, громадськості, функціонування об'єктів критичної інфраструктури (медичні заклади, заклади зв'язку, транспорту, енергетики, банківсько-фінансової сфери тощо) та ін., то сьогодні безперебійна реалізація ними своїх завдань, що виключає ризики і загрози, пов'язані з кіберпростором, неможлива без звернення до послуг аутсорсингу інформаційної безпеки. Тому умовою реалізації цього напряму є розробка й реалізація політики інформаційної безпеки, заснованої на професійному захисті інформаційним ресурсів, що належать тим чи іншим суб'єктам, при достатньому фінансуванні подібної діяльності. Вочевидь, настав час не лише для проведення постійних інструктажів, консультацій та інформування працівників, робота яких організована в режимі он-лайн, щодо безпечної віддаленої взаємодії особистих інформаційно-обчислюваних агрегатів із комп'ютерною технікою кампаній, а й для виключення будь-якої можливості експлуатації віддалених вузлів із боку сторонніх осіб, насамперед зловмисників, а так само для організації надійної системи захищеного доступу з віддалених комп'ютерів до серверів з використанням, наприклад, засобів криптографічного кодування інформації, блокування сеансів віддаленого доступу користувачів понад установлений для роботи час та ін. Також своєрідним *modus operandi* має стати застосування користувачами, що працюють на віддаленій інформаційно-обчислюваній техніці, програм антивірусного захисту

інформації, актуальність і надійність яких не втрачаються завдяки щоденному оновленню. В умовах тривання карантинних заходів не зайвим буде визначити чітку номенклатуру інформаційних ресурсів і розміщеної на серверах кампаній інформації, доступ до яких має характер віддаленого. В ідеалі працівникам на віддаленому режимі роботи для реалізації ними своїх функціональних обов'язків кампаніями на відповідний період доцільно видавати комп'ютерну техніку (планшети, ноутбуки, комп'ютери, мобільні засоби зв'язку тощо), що має надійний захист.

Кібербезпека для пересічних громадян в інформаційному просторі повинна міцно асоціюватися з інформаційною гігієною. Трьома «китами» зазначеної гігієни в кіберпросторі сьогодні можна вважати, по-перше, максимальне інформування громадян з приводу небезпек, що містить в собі «спілкування» з високими інформаційними технологіями; по-друге, максимальне обмеження будь-якої інформації про себе, що залишається людиною в інформаційних мережах і навіть при зверненні в різноманітні соціальні інституції; по-третє, заборону на прийняття наполегливих пропозицій перейти за посиланням на невідомі сайти або відкрити листи від незнайомих принаймні осіб або організацій. Так, завдяки нескладним порадам у людини рано чи пізно виробиться звичка, прикладом, використовувати ліцензійне програмне забезпечення та періодично оновлювати операційну систему. Водночас стане за правило вдаватися до системи резервного копіювання інформації та, навпаки, пам'ятати про засоби гарантованого стирання даних, а також не користуватися безкоштовними Wi-Fi мережами без незахищеного з'єднання, адже користування саме таким сервісом таїть у собі ризик втрати важливих персональних даних через дії недобросовісних адміністраторів подібних мереж. Дотримуватися цього нескладного правила зовсім не важко для активних користувачів, якими переважно є молоді особи та особи середнього віку. Крім того, останнім часом чимало соціальних мереж, особистих кабінетів у різноманітних

електронних сервісах йдуть шляхом вдосконалення системи доступу (ускладнені комбінації символів та їх періодична зміна, ідентифікація користувачів у кілька етапів та ін.), що покликано забезпечувати додатковий захист персональних даних користувачів. Такий підхід має стати звичайною практикою убезпечення персональних даних від дій зловмисників, що до того ж із порозумінням повинно сприйматися користувачами. І, напевно, найпростіше правило-пересторога: користувачі Інтернет-мереж у будь-якому разі мають звертатися до перевірених джерел для отримання необхідної інформації (особливо якщо це стосується стану та перспектив боротьби із коронавірусною хворобою).

Дослідження тенденцій кіберзлочинності карантинного періоду та аналіз можливостей протидії їй дозволяє зробити кілька висновків.

По-перше, помітними тенденціями в період запровадження й реалізації карантинних заходів у зв'язку з поширенням у світі пандемії COVID-19 є: небувале збільшення кількості кіберзлочинів у світі; «експлуатація» стурбованості людей ситуацією із коронакризою та її наслідками, через що весь масив цих злочинів так чи інакше корелює з пандемією; розширення об'єктів кібератак та перенесення акцентів на те, в який саме спосіб «ефективніше» втручатися в роботу інформаційно-комунікаційних приладів; виникнення так званого пандемічного злочинця-шахрая; створення серйозної загрози з боку кіберзлочинців для сфери охорони здоров'я та ін.

По-друге, особливо слід наголосити на тому факті, що пандемія COVID-19 «посприяла» виникненню у кримінальному світі нового феномену – пандемічного злочинця, протиправна поведінка якого знаходить свій проявів перш за все в інформаційному просторі. У подальшому вивченню цього феномену та моніторингу його трансформації має відводитися окрема увага в межах пізнання явища кіберзлочинності.

По-третє, з'ясування новітніх тенденцій в «онтології» кіберзлочинності призводить до розуміння необхідності зміни стратегії протидії кіберзагрозам

із «традиційної» наступальної на оборонну, в якій пріоритет віднині має віддаватися саме захисту інформації від можливих загроз. Це зумовлюється багатьма факторами, серед яких, зокрема, сучасний формат спілкування, характер виробничих процесів і ведення бізнесу, стирання кордонів між корпоративними та особистими інформаційно-комунікаційними пристроями, залежність інформаційної безпеки від людського фактору, необхідність пошуку додаткових джерел для забезпечення інформаційної безпеки тощо.

По-четверте, головними напрямами оборонної стратегії, спрямованої проти кіберзлочинів, слід визнати: 1) розробку й реалізацію політики інформаційної безпеки як окремих суб'єктів інформаційного простору, так й суспільства, держави в цілому; 2) інформаційну просвіту щодо тематики, яку найчастіше експлуатують зловмисники у періоди епідемій, пандемій та інших природних і соціальних катаклізмів, та конкретних заходів інформаційної безпеки; 3) розвиток ринку послуг аутсорсингу інформаційної безпеки; 4) формування навичок дотримання інформаційної гігієни пересічних громадян у кіберпросторі; 5) постійний моніторинг і наукові дослідження проблем цифровізації соціуму тощо.

Список використаних джерел

1. 134. Cybersecurity Statistics and Trends for 2021/ https://www.varonis.com/blog/cybersecurity-statistics/ (дата звернення: 08.06.2021).

2. Cybercrime and COVID-19: Risks and Responses. https://www.unodc.org/documents/Advocacy-Section/EN_-UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf (дата звернення: 30.06.2021).

3. Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis. URL: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis. (дата звернення: 30.06.2021).

4. 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.

5. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження. URL: https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766 (дата звернення: 21.06.2021).

6. Ключевская Н. Информационная безопасность и COVID-19: рекомендации для бизнеса и граждан. URL: https://www.garant.ru/article/1421147/ (дата звернення: 20.06.2021).

7. Коронавирус COVID-19: общая статистика. URL: https://index.minfin.com.ua/reference/ coronavirus/ (дата звернення: 07.07.2021).

8. Лефтеров Л. В. Запобігання підрозділами Національної поліції шахрайству, що вчиняється з використанням засобів електронних комунікацій: автореф. дис. ... канд. юрид. наук: 12.00.08 / Одес. держ. ун-т внутр. справ. Одеса, 2019. 20 с.

9. 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: 21.06.2021).

10. Моисеев А. А. Условия и последствия диджитализации современного общества: социально-экономический анализ. *Вестник Томского государственного университета. Философия. Социология. Политология.* 2017. № 39. С. 216–226.

11. Про внесення змін до деяких законодавчих актів України, спрямованих на запобігання виникненню і поширенню коронавірусної хвороби (COVID-19): Закон України від 17 березня 2020 р. № 530-IX. *Відомості Верховної Ради України.* 2020. № 16. Ст. 100.

12. Про встановлення карантину з метою запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, та етапів послаблення протиепідемічних заходів: постанова Кабінету Міністрів України від 20 травня 2020 р. № 392. *Урядовий кур'єр*. 2020. 21 трав. № 95.

13. Про встановлення карантину та запровадження обмежувальних протиепідемічних заходів з метою запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2: постанова Кабінету Міністрів України від 09 грудня 2020 р. № 1236. *Урядовий кур'єр*. 2020. 12 груд. № 243.

14. Про встановлення карантину та запровадження посилених протиепідемічних заходів на території із значним поширенням гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2: постанова Кабінету Міністрів України від 22 липня 2020 р. № 641. *Урядовий кур'єр*. 2020. 25 лип. № 142.

15. Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2: постанова Кабінету Міністрів України від 11 березня 2020 р. № 211. *Урядовий кур'єр*. 2020. 12 берез. № 47.

16. Про захист населення від інфекційних хвороб: Закон України від 6 квітня 2000 р. № 1645-III. https://zakon.rada.gov.ua/laws/show/1645-14#Text (дата звернення: 30.06.2021).

17. Романов М. В. Цифровізація і забезпечення прав людини під час пандемії COVID-19. *Забезпечення правопорядку в умовах коронакризи:* матеріали панельної дискусії IV Харків. міжнар. юрид. форуму, м. Харків, 23–24 верес. 2020 р. / редкол.: В. Я. Тацій, А. П. Гетьман, Ю. Г. Барабаш, Б. М. Головкін. Харків: Право, 2020. С. 181–187.

18. Стрій Є. Don't click shit! Як вберегтися від кіберзлочинців у час пандемії. URL: https://investigator.org.ua/ua/publication/224967/ (дата звернення: 21.06.2021).

19. Текущая статистика по коронавирусу на 7.07.2021 (Украина). URL: https://index.minfin.com.ua/reference/coronavirus/ukraine/ (дата звернення: 07.07.2021).

20. У 2020 році Нацполіція викрила більше ніж 5 000 кіберзлочинів. URL: https://www.kmu.gov.ua/news/u-2020-mu-nacpoliciya-vikrila-ponad-5-000-kiberzlochiniv (дата звернення: 10.06.2021).

REFERENCES

1. 134. Cybersecurity Statistics and Trends for 2021/ https://www.varonis.com/blog/cybersecurity-statistics/ [in English].

2. Cybercrime and COVID-19: Risks and Responses. https://www.unodc.org/documents/Advocacy-Section/EN_-UNODC_-_CYBERCRIME_ AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf [in English].

3. Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis. URL: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis [in English].

4. Kalinina, A. V. (2020). Pandemiya virusu vs pravoporyadok: kriminologichnij prognoz. *Pitannya borot`bi zi zlochinnistyu: zb. nauk. pr., 39, 39–45* [in Ukrainian].

5. Kiberzlochinczi u 2020 roczi zavdali u sviti` zbitkiv na tril`jon dolariv – doslidzhennya. URL: https://www.dw.com/uk/kiberzlochyny-u-2020-rotsi-zavdaly-svitu-zbytkiv-na-trylion-dolariv-doslidzhennia/a-55857766 [in Ukrainian].

6. Klyuchevskaya N. Informaczionnaya bezopasnost` i COVID-19: rekomendaczii dlya biznesa i grazhdan. URL: https://www.garant.ru/article/1421147/ [in Russian].

7. Koronavirus COVID-19: obshhaya statistika. URL: https://index.minfin.com.ua/reference/ coronavirus/ [in Russian].

8. Lefterov, L. V. (2019) Zapobigannya pidrozdilami Naczional`noyi policziyi shakhrajstvu, shho vchinyayet`tsya z vikoristannyam zasobiv elektronnikh komunikaczij. *Candidate's thesis.* Odesa [in Ukrainian].

9. Markov A. Informaczionnaya bezopasnost` v usloviyakh pandemii COVID-19. URL: https://expert.ru/2020/04/9/informatsionnaya-bezopasnost-v-usloviyah-pandemii-covid-19/ [in Russian].

10. Moiseev, A. A. (2017). Usloviya i posledstviya didzhitalizaczii sovremennogo obshhestva: soczial`no-ekonomicheskij analiz. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Socziologiya. Politologiya, 39, 216-226* [in Russian].

11. Pro vnesennya zmin do deyakikh zakonodavchikh aktiv Ukrayiny, spryamovanikh na zapobigannya viniknennyu i poshirennyu koronavirusnoyi khvoroby (COVID-19): Zakon Ukrayiny vid 17 bereznya 2020 r. # 530-IX (2020). *Vidomosti Verkhovnoyi Rady Ukrayiny, 16, art. 100* [in Ukrainian].

12. Pro vstanovlennya karantinu z metoyu zapobigannya poshirennyu na teritoriyi Ukrayiny gostroyi respiratornoyi khvorobi COVID-19, sprichinenoyi koronavirusom SARS-CoV-2, ta etapiv poslablennya protiepidemichnykh zakhodiv: postanova Kabinetu Ministriv Ukrayiny vid 20 travnya 2020 r. # 392 (2020). *Uryadovij kur'yer, 21 trav., art. 95* [in Ukrainian].

13. Pro vstanovlennya karantinu ta zaprovadzhennya obmezhuval`nykh protiepidemichnykh zakhodiv z metoyu zapobigannya poshirennyu na teritoriyi Ukrayiny gostroyi respiratornoyi khvoroby COVID-19, sprichinenoyi koronavirusom SARS-CoV-2: postanova Kabinetu Ministriv Ukrayiny vid 09 grudnya 2020 r. # 1236 (2020). *Uryadovij kur'yer, 12 grud., art. 243* [in Ukrainian].

14. Pro vstanovlennya karantinu ta zaprovadzhennya posilenykh protiepidemichnykh zakhodiv na teritoriyi iz znachnim poshirennyam gostroyi respiratornoyi khvoroby COVID-19, sprichinenoyi koronavirusom SARS-CoV-2: postanova Kabinetu Ministriv Ukrayiny vid 22 lipnya 2020 r. # 641 (2020). *Uryadovij kur'yer, 25 lip., art.142* [in Ukrainian].

15. Pro zapobigannya poshirennyu na teritoriyi Ukrayiny gostroyi respiratornoyi khvoroby COVID-19, sprichinenoyi koronavi`rusom SARS-CoV-2: postanova Kabinetu Ministriv Ukrayiny vid 11 bereznya 2020 r. # 211 (2020). *Uryadovij kur'yer, 12 berez., art. 47* [in Ukrainian].

16. Pro zakhist naselennya vid infekczijnykh khvorob: Zakon Ukrayiny vid 6 kvitnya 2000 r. # 1645-III. URL: https://zakon.rada.gov.ua/laws/show/1645-14#Text [in Ukrainian].

17. Romanov, M. V. (2020). Czifrovizacziya i zabezpechennya prav lyudiny pid chas pandemiyi COVID-19. *Zabezpechennya pravoporyadku v umovakh koronakrizi:* materiali panel`noyi diskusiyi IV Kharkiv. mizhnar. yurid. forumu, m. Kharki`v, 23–24 veres. 2020 r. / redkol.: V. Ya. Taczij, A. P. Get`man, Yu. G. Barabash, B. M. Golovkin. Kharkiv: Pravo, *181–187* [in Ukrainian].

18. Strij Ye. Don't click shit! Yak vberegtisya vid kiberzlochincziv u chas pandemiyi. URL: https://investigator.org.ua/ua/publication/224967/ [in Ukrainian].
19. Tekushhaya statistika po koronavirusu na 7.07.2021 (Ukraina). URL: https://index.minfin.com.ua/reference/coronavirus/ukraine/ [in Russian].
20. U 2020 roczi` Naczpolicziya vikryla bil`she nizh 5 000 kiberzlochiniv. URL: https://www.kmu.gov.ua/news/u-2020-mu-nacpoliciya-vikrila-ponad-5-000-kiberzlochiniv [in Ukrainian].

Батыргареева В. С. Основные тенденции киберпреступности карантинного периода и противодействие ей

В статье проанализированы новейшие тенденции киберпреступности во время введения и реализации карантинных мер в связи с распространением в мире пандемии COVID-19 и некоторые последствия данного вида преступности. Приведены причины, которые привели к появлению в криминальной среде нового феномена – так называемого пандемического преступника, противоправное поведение которого находит проявление прежде всего в информационном пространстве. Отмечены опасности киберпреступности для объектов критической инфраструктуры, среди которых особый акцент делается на учреждениях здравоохранения. Раскрыта концептуальная идея противодействия киберпреступности, содержание которой будет определять и стратегические направления этого противодействия на современном этапе развития общества.

Ключевые слова: *информационное пространство, пандемия COVID-19 «пандемический преступник», киберпреступность, противодействие.*

Batyrgareieva V. S. The main trends of cybercrime in the quarantine period and counteraction to it

The article analyzes the latest trends in cybercrime during the introduction and implementation of quarantine measures in connection with the spread of the COVID-19 pandemic in the world and the consequences of this type of crime. Such trends include: a significant increase in the number of cybercrimes in the world and in Ukraine; «exploitation» by criminals of people's concerns about the situation with the coronary crisis and its negative consequences, as a result of which the whole array of these crimes somehow correlates with the pandemic; expanding the objects of cyberattacks and shifting the emphasis on how to «more effectively» interfere in the work of information and communication devices; the emergence of the so-called pandemic offender; creating a serious threat from cybercriminals to the health sector, etc. The whole array of cybercrimes is divided into offenses, in the «scenario» of which the coronavirus theme is decisive, and «traditional» cybercrimes, the committing of which is not directly conditioned by this event, although the number of such crimes (increasing) correlates with special pandemic conditions. The article presents the reasons that led to the emergence of a new phenomenon in the criminal world – a pandemic criminal, whose illegal

behavior is manifested primarily in the information space. The danger of cybercrime for the lens of critical infrastructure is emphasized, with special emphasis on medical facilities. The conceptual idea of counteracting cybercrime is revealed, which consists in changing the strategy of counteracting cyber threats from «traditional» offensive to defensive, in which the priority should be given to the protection of information from possible threats. This is due to many factors, including the modern format of communication, the nature of production processes and business, blurring the boundaries between corporate and personal information and communication devices, the dependence of information security on the human factor, the need to find additional sources for information security. The content of the defense strategy of counteraction will determine the strategic directions of this counteraction. The main directions of the defense strategy are: 1) development and implementation of information security policy as individual subjects of the information space, and society, the state as a whole; 2) information education on topics that are most often exploited by criminals during epidemics, pandemics and other natural and social cataclysms, and specific information security measures; 3) development of the market of information security outsourcing services; 4) formation of skills of observance of information hygiene of ordinary citizens in cyberspace; 5) constant monitoring and research of problems of digitalization of society; etc.

Keywords: *information space, pandemic COVID-19, «pandemic offender», cybercrime, counteraction.*