УДК 343.322
DOI https://doi.org/10.32782/2524-0374/2022-5/118

АНАЛІЗ ЗАКОНОДАВЧИХ ЗМІН, НАПРАВЛЕНИХ НА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИМІНАЛЬНО-ПРАВОВОЇ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ДІЇ ВОЄННОГО СТАНУ

ANALYSIS OF LEGISLATIVE CHANGES AIMED AT IMPROVING THE EFFECTIVENESS OF CRIMINAL LAW COUNTERACTING CYBERCRIME IN WARTIME CONDITIONS

Мовчан Р.О., д.ю.н., професор,
професор кафедри конституційного, міжнародного і кримінального права
Донецький національний університет імені Василя Стуса

У статті проаналізовано кримінально-правові наслідки ухвалення Закону України від 24 березня 2022 р.№ 2149-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану». Зокрема, проведене дослідження дало можливість сформулювати авторські рекомендації щодо вирішення найбільш складних правозастосовчих проблем, а також запропонувати зміни до Кримінального кодексу України, направлені на усунення вад аналізованого Закону, ухвалення яких сприятиме досягненню вищої ефективності відповідних кримінально-правових приписів.

Піддано критиці положення про те, що для кваліфікації відповідних посягань за ч. 5 ст. 361 КК не вимагається того, щоб вони скоювалися «з використанням умов воєнного стану», а натомість достатньо їхнього вчинення в умовах воєнного стану і спричинення наслідків, передбачених ч. 3 або ч. 4. Резюмується, що прямим результатом такого законодавчого кроку стало те, що відтепер, наприклад, банальний, але вчинюваний в умовах воєнного часу несанкціонований перегляд телепередач має отримувати кримінально-правову оцінку з посиланням саме на ч. 5 ст. 361 КК.

Висувається гіпотеза відносно невиправданої суворості і передбачених санкціями і більшості інших частин ст. 361 КК покарань.

Доведено недоцільність пов'язування посилення відповідальності за несанкціоноване втручання як зі «створенням небезпеки тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків» (ч. 4 ст. 361 КК), так і з «вчиненням під час дії воєнного стану» (ч. 5 ст. 361 КК).

Аргументується помилковість вилучення існуючого раніше у примітці ст. 361 КК принципово важливого застереження відносно того, що при оцінці «значної шкоди» згаданий майновий еквівалент мав братися до уваги лише тоді, коли така шкода полягала у заподіянні матеріальних збитків, який призвів до суттєвого та нічим невиправданого звуження сфери потенційного застосування ч. 4 ст. 361 КК.

Ключові слова: несанкціоноване втручання, воєнний стан, інформаційні системи, інформація, кіберзлочин, диверсія.

The article analyzes the criminal law consequences of the adoption of the Law of Ukraine dated March 24, 2022 No. 2149-IX "On Amendments to the Criminal Code of Ukraine on Improving the Effectiveness of Combating Cybercrime under Martial Law". In particular, the study made it possible to formulate the author's recommendations for solving the most complex law enforcement problems, as well as to propose changes to the Criminal Code of Ukraine aimed at eliminating the shortcomings of the Law under consideration, the adoption of which will contribute to the achievement of the highest efficiency of the relevant criminal law prescriptions.

Criticized the position that in order to qualify the relevant encroachments under Part 5 of Art. 361 of the Criminal Code, it is not required that they be committed "using the conditions of martial law", but it is enough to commit them under martial law and inflict the consequences provided for in part 3 or part 4. It is summarized that the direct result of such a legislative step was that now, for example, banal, but unauthorized viewing of television programs committed in wartime conditions should receive a criminal legal assessment with reference to Part 5 of Art. 361 of the Criminal Code.

A hypothesis is put forward regarding the unjustified severity and sanctions provided for by most other parts of Art. 361 of the Criminal Code of punishments.

The inexpediency of linking increased responsibility for unauthorized interference with both "creating the danger of severe technological accidents or environmental disasters, death or mass illness of the population or other serious consequences" (part 4 of article 361 of the Criminal Code), and with "commission during martial law "(part 5 of article 361 of the Criminal Code).

The erroneousness of the withdrawal of the previously existing in the footnote Art. 361 of the Criminal Code of a fundamentally important reservation that when assessing "significant damage", the mentioned property equivalent should be taken into account only when such damage consisted in causing material damage, which led to a significant and unjustified narrowing of the scope of potential application of Part 4 of Art. 361 of the Criminal Code.

Key words: unauthorized interference, martial law, information systems, information, cybercrime, sabotage.

Перш ніж оголосити про проведення «спеціальной опєрації» та перейти до відкритого використання танків, артилерії, авіації, одурманених пропагандою солдат тощо, росія ще протягом кількох тижнів перед 24 лютим 2022 р. широко вдавалася і до застосування іншої форми агресії – масштабних кібератак проти нашої держави, призначенням яких було не лише втручання в роботу об'єктів критичної інфраструктури, а й поширення панічних настроїв серед українців. Вже дещо з іншими цілями, але відповідні кібератаки продовжились і після початку активної фази бойових дій та введення воєнного стану.

Зважаючи на ці обставини, у стінах Верховної Ради України був розроблений та зареєстрований законопроєкт (№ 7182 від 20 березня 2022 р.), мета якого була задекларована як «посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі». А вже 24 березня 2022 р. відповідний законопроєкт набув статусу Закону України № 2149-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» (далі – Закон від 24 березня 2022 р.).

Потребою доктринального осмислення відповідних нормативних приписів і викликана необхідність проведення представленого дослідження.

Метою цієї статті є:

– по-перше, викладення власного бачення щодо тих дискусійних положень аналізованих Законів, опанування яких здатне викликати найбільші складнощі як у пересічних громадян, так і у правозастосовців. Ці рекомендації будуть розміщені в рубриці «Що слід враховувати громадянам та правозастосовцям»;

– по-друге, виявлення та висловлення пропозицій щодо усунення притаманних згаданим Законам вад, наявність яких може негативно позначитися на результативності ст. 114-2 КК. Ці питання будуть розглянуті в межах

іншої умовної рубрики – «Що не врахував законодавець».

Результатом ухвалення Закону від 24 березня 2022 р. стало одночасне внесення змін до двох норм КК – статей 361 та 361-1.

Зокрема, в обох цих заборонах відтепер вказується на те, що несанкціоноване втручання (у ст. 361 КК воно виступає формою суспільно небезпечного діяння, а у ст. 361-1 КК – призначенням шкідливих програмних чи технічних засобів) здійснюється в роботу **«інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»**, замість втручання у передбачені раніше «електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку». Вочевидь таке уточнення слід пов'язувати із бажанням вітчизняних парламентаріїв узгодити відповідну термінологію із тією, яка використовується у прийнятому ще 16 грудня 2020 р. Законі України «Про електронні комунікації» (він прийшов на зміну Закону України «Про телекомунікації», котрий втратив чинність якраз таки через ухвалення попереднього).

Та попри озвучені намагання щодо «узгодження», слід констатувати, що, наприклад, для тлумачення понять «інформаційна (автоматизована)» та «інформаційно-комунікаційна система» необхідно звертатися до положень іншого нормативно-правовому акту, а саме, Закону України «Про захист інформації в інформаційно-комунікаційних системах». Легальної ж дефініції зворотів «електронні комунікаційні системи» чинним законодавством, наскільки відомо автору цих рядків, не передбачено; натомість у Законі України «Про електронні комунікації» надаються визначення «електронних комунікаційних мереж», «електронних комунікаційних послуг» та «електронних комунікацій».

Крім цього уточнення, в іншому ст. 361-1 КК зазнала лише незначного корегування, яке виявилося у:

– по-перше, вказівці в її назві та диспозиції ч. 1 на те, що створення шкідливих програмних чи технічних засобів є караним за відповідною нормою лише тоді, коли воно вчиняється з метою «протиправного» використання, розповсюдження або збуту, яка (протиправність) раніше хоча й припускалась, однак пряме згадування про котру було відсутнє;

– по-друге, незначному посиленні відповідальності за дії, передбачені все тією ж ч. 1.

Натомість куди серйозніших змін зазнала ст. 361 КК, відповідно до оновленої редакції якої:

1) кримінально протиправним визнається сам факт несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (з мотивів зручності далі у цій публікації для позначення відповідного кримінального правопорушення вживатиметься єдиний зворот «несанкціоноване втручання») – незалежно від того, чи призвели такі дії до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, настання яких відтепер повинно вважатися не криміноутворюючою (як раніше), а кваліфікуючою ознакою розглядуваного кримінального правопорушення (далі – к. пр.) (нова ч. 3 ст. 361 КК).

Коментуючи відповідні зміни, М. І. Хавронюк висловлює припущення відносно того, що тут має місце надмірна криміналізація, адже, на думку вченого, саме по собі несанкціоноване втручання в роботу згаданих систем чи мереж не є к. пр., оскільки не створює жодних наслідків, які можна було б охопити поняттям істотної шкоди (ст. 11 КК). При цьому в якості прикладу моделюється ситуація, коли колега по роботі бажає подивитися новини з використанням ПК іншого працівника, поки свій в ремонті, включає його і робить пошук на сайтах (малозначне діяння) [1].

Частково погоджуючись із аргументами науковця, водночас зауважу, що, як на мене, питання про обґрунтованість криміналізації згаданих діянь може бути вирішено тільки за результатами проведення окремого дослідження, у межах якого було б:

а) чітко визначено суспільну небезпеку несанкціонованого втручання, «ціна» якого як посягання на приватність життя, з урахуванням всеосяжної діджиталізації суспільства, з кожним днем лише зростає;

б) детально проаналізовано відповідний іноземний досвід. Зокрема, навіть не занурюючись у вивчення цієї проблематики, все ж хотів би звернути увагу на тому, що парламентарії принаймні декількох європейських країн оцінюють суспільну небезпеку несанкціонованого втручання в роботу інформаційних систем таким чином, що визнають це діяння кримінально протиправним – або ж безумовно, або ж за умови супроводження цих дій подоланням (порушенням) заходів безпеки – незалежно від жодних його наслідків (див., наприклад: ст. 118-а КК Австрії, ст. 217 Пенітенціарного кодексу Естонії, ч. 3 ст. 197 КК Іспанії, ст. 138 КК Нідерландів, ст. 267 КК Польщі тощо);

в) враховано міжнародні зобов'язання України. Зокрема, у ст. 2 Конвенції Ради Європи про кіберзлочинність (ратифікована Україною у 2005 р.) передбачена необхідність криміналізації незаконного доступу, тобто умисний доступ до цілої комп'ютерної системи або її частини без права на це. Кримінальна відповідальність в цьому випадку не пов'язується з будь-якими наслідками. Водночас слід ураховувати, що в цій же нормі вказується на те, що країна може вимагати, щоб таке правопорушення було вчинене шляхом порушення заходів безпеки з метою отримання комп'ютерних даних або з іншою недобросовісною метою, або по відношенню до комп'ютерної системи, поєднаної з іншою комп'ютерною системою;

2) посилено відповідальність:

– по-перше, за дії, передбачені ч. 1 або ч. 2, які створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків (нова ч. 4);

– по-друге, за дії, передбачені ч. 3 або ч. 4, вчинені під час воєнного стану (нова ч. 5);

3) дії, передбачені частинами 1–4 цієї статті, відтепер не вважаються несанкціонованим втручанням, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж (нова ч. 6).

На жаль, як і в ситуації з більшістю інших «воєнних» змін до КК, далеко не всі оновлення, пов'язані з ухваленням Закону від 24 березня 2022 р. (у тому числі й згадані вище), слід оцінювати позитивно.

Розпочну із найбільш актуального – посилення відповідальності за вчинення розглядуваних діянь саме «під час дії воєнного стану» (ч. 5 ст. 361 КК). Як бачимо, для кваліфікації відповідних посягань за цією нормою не вимагається того, щоб вони скоювалися «з використанням умов воєнного стану», а натомість достатньо їхнього вчинення в умовах воєнного стану і спричинення наслідків, передбачених ч. 3 або ч. 4.

Прямим результатом такого законодавчого кроку стало те, що відтепер, наприклад, банальний, але вчинюваний в умовах воєнного часу перегляд телепередач (як і інші подібні дії) за допомогою несанкціонованого підключення свого кабелю до відповідних мереж, прояви якого якраз таки і складали левову долю правопорушень, які кваліфікувалися за ст. 361 КК, має отримувати кримінально-правову оцінку з посиланням саме на ч. 5 ст. 361 КК, санкцією якої передбачено безальтернативне основне покарання у виді позбавлення волі на строк від 10 до 15 років (!!!).

Тож чи є підстави вважати таке покарання адекватним, особливо якщо пригадати, що, скажімо:

– умисне тяжке тілесне ушкодження, вчинене способом, що має характер особливого мучення, або таке, що спричинило смерть потерпілого (ч. 2 ст. 121 КК), карається позбавленням волі на строк лише від 7 до 10 років;

– некваліфікований теракт (ч. 1 ст. 258 КК) – позбавленням волі на строк лише від 5 до 10 років;

– та навіть некваліфіковане умисне убивство (ч. 1 ст. 115 КК) – позбавленням волі на строк лише від 7 до 15 років?

Як бачимо, «завдяки» аналізованому рішенню несанкціонований перегляд футболу в умовах воєнного стану має вважатися на порядок небезпечнішим за вчинені у цей же часовий період умисне вбивство, умисне тяжке тілесне ушкодження, що спричинило смерть потерпілого, і навіть за вчинений в умовах воєнного стану розбій (ч. 4 ст. 187 КК), покарання за який є менш суворим (позбавлення волі на строк від 8 до 15 років) навіть з урахуванням здійсненого нещодавно (див. Закон № 2117-IX) посилення відповідальності за ці дії.

Та й загалом висуну гіпотезу відносно того, що передбачені санкціями і більшості інших частин ст. 361 КК є занадто та невиправдано суворими, що, зокрема, виявляється у вказівці у них на покарання у виді позбавлення волі на досить тривалі терміни.

Наприклад, за жодних умов не можу підтримати передбачену санкцією ч. 3 ст. 361 КК саму можливість призначення за той таки банальний, не пов'язаний із завданням значної шкоди несанкціонований перегляд футбольних матчів покарання у виді позбавлення волі на строк від 3 до 8 років. Тут знову доречно пригадати покарання, встановлені за вчинення багатьох інших і очевидно небезпечніших діянь, зокрема за:

– посягання на територіальну цілісність і недоторканність України (ч. 1 ст. 110 КК);

– або фінансування дій, вчинених з метою зміни меж території або державного кордону України (ч. 1 ст. 110-2 КК), які (як перше, так і друге) можуть каратися позбавленням волі на строк лише від 3 до 5 років;

– або ж, скажімо, за вимагання, поєднане з погрозою вбивства (ч. 2 ст. 189 КК – позбавлення волі на строк від 3 до 5 років).

А ось на адресу конструювання ч. 4 ст. 361 КК, в якій, як ми пам'ятаємо, встановлено відповідальність за дії, передбачені ч. 1 або ч. 2 цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, хотілося б висловити зауваження як подібного до попереднього, так і дещо іншого характеру.

По-перше, знову привертає до себе увагу невиправдано суворе основне покарання, встановлене за вчинення розглядуваних діянь – позбавлення волі на строк від 8 до 12 років. І це, укотре підкреслю, за дії, які призвели:

– або ж до матеріальної шкоди, яка лише (доцільність такої характеристики пояснюється згаданою суворістю покарання) в 300 і більше разів перевищує НМДГ;

– або ж лише до створення небезпеки настання певних наслідків.

Для того, щоб наочніше продемонструвати несправедливість існуючого стану речей, знову звернуся до порівняння відповідного покарання із покараннями, встановленими за вчинення деяких інших к. пр., які призвели до таких самих або вищих матеріальних наслідків, зокрема із:

– порушенням авторського права і суміжних прав, яке завдало матеріальну шкоду в розмірі 1 тис. і більше НМДГ (ч. 3 ст. 176 КК), найсуворішим покаранням за яке є позбавлення волі на строк від 3 до 6 років;

– крадіжкою чи шахрайством на суму в 600 та більше НМДГ (ч. 5 ст. 185 КК та ч. 4 ст. 190 КК, відповідно) – позбавлення волі на строк від 7 (5) до 12 років;

– протидією законній господарській діяльності, що заподіяла шкоду, яка в 500 і більше разів перевищує НМДГ (ч. 3 ст. 206 КК) – позбавлення волі на строк від 6 до 10 років тощо.

Як бачимо, незважаючи на очевидний і, на мою думку, не потребуючий доведення факт того, що кожне із цих к. пр. є принаймні не менш небезпечним, аніж передбачене ч. 4 ст. 361 КК, а відповідальність за їхнє вчинення пов'язується навіть з вищими показниками НМДГ, всі вони караються менш суворо, аніж розглядуваний делікт.

Ну й нарешті зазначу, що попри все своє різноманіття, у чинному КК існує лише одна стаття, в якій кримінальна відповідальність пов'язується із настанням саме тих наслідків, про які згадується у ч. 4 ст. 361 КК, – це ст. 253 КК «Проектування чи експлуатація споруд без систем захисту довкілля». При цьому відповідні дії, які, як і в аналізованій нормі, лише створили небезпеку згаданих наслідків (ч. 1), караються штрафом від 1 тис. до 3 тис. НМДГ; у випадку ж реального настання таких наслідків (ч. 2) має призначатися покарання у виді обмеження волі на строк від 3 до 5 років або позбавлення волі на строк до 5 років.

Через це знову виникає питання: невже відповідне несанкціоноване втручання, яке призвело лише до створення небезпеки загибелі людей (ч. 4 ст. 361 КК), є більш ніж удвічі небезпечнішим за проектування споруд без систем захисту довкілля, яке призвело до реальних наслідків у виді смерті багатьох людей (ч. 2 ст. 253 КК)?

По-друге (це зауваження безпосередньо стосується попереднього прикладу), виникає і питання відносно того, а чим саме керувався законодавець, пов'язуючи посилення відповідальності за кіберзлочин із загрозою настання саме згаданих вище наслідків, які є характерними, а тому й згадуються насамперед при описанні складів к. пр. проти довкілля, безпеки виробництва, а також (хоча й дещо меншою мірою) громадської безпеки та безпеки руху і експлуатації транспорту.

У зв'язку зі змістом (сутністю) діяння, про яке йдеться у ст. 361 КК, подібне питання можна поставити і щодо доцільності диференціації відповідальності за його вчинення під час дії воєнного стану (ч. 5 ст. 361 КК), яка (доцільність), зважаючи саме на характер суспільної небезпеки розглядуваного діяння, не виглядає доволі очевидною.

Однак уважний читач напевно може поставити зустрічне питання: а чи не забув я про свої викладені ще на початку цієї статті слова про постійні кібератаки з боку росії, до котрих так само апелювали і розробники Закону від 24 березня 2022 р., і які:

– очевидно є куди більш небезпечнішими саме під час дії воєнного стану;

– можуть мати на меті і, враховуючи існуючу сьогодні тотальну діджиталізацію усіх сфер життя, теоретично спроможні призвести до наслідків найрізноманітнішого характеру, зокрема й тих, на загрозу настання яких вказується в ч. 4 ст. 361 КК.

Проте, випереджаючи це питання, я відразу дам на нього відповідь: ні, у сучасних воєнних умовах про ці обставини я просто не міг забути і, навпаки, увесь час їх ураховую.

Мій же скептицизм стосовно доцільності передбачення відповідних кваліфікуючих ознак досліджуваного к. пр. насамперед пояснюється тим, що, спочатку уважно проаналізувавши, а потім синтезувавши всю попередню інформацію, я звернув увагу на те, що:

– по-перше, всі кібератаки рф, про які у супровідних документах вели мову автори Закону від 24 березня 2022 р., вчинялися і вчиняються лише з однією ціллю – ослабити нашу державу, тобто тією метою, яка є обов'язковою криміноутворюючою і, власне, визначальною конститутивною ознакою передбаченої ст. 113 КК диверсії;

– по-друге, згадані у розглядуваній забороні потенційні наслідки у вигляді «тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків» фактично повністю охоплюються тими наслідками, з метою спричинення яких і вчиняється та ж таки диверсія – «масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій».

Отже, можна констатувати, що відповідні кібератаки рф, які вчиняються для спричинення наслідків, передбачених у ч. 4 ст. 361 КК, насправді є нічим іншим, як однією з форм диверсії, яка за «звичайних» умов має кваліфікуватися за ч. 1 ст. 113 КК, а за умов вчинення в умовах воєнного стану або в період збройного конфлікту – за ч. 2 ст. 113 КК.

Звісно, загроза настання передбачених ч. 4 ст. 361 КК наслідків несанкціонованого втручання може мати місце і тоді, коли не була метою останнього, що виключає можливість інкримінування ст. 113 КК. Однак, оцінюючи подібну можливість, хотілося б зауважити те, що:

– по-перше, стосовно більшості із відповідних наслідків вона є суто теоретичною;

– по-друге, якщо ж загроза відповідних наслідків, які не були метою втручання, все ж настала, то чи виправдано призначати за таке к. пр. покарання у виді позбавлення волі на строк від 8 до 12 років?

– по-третє, враховуючи сутність несанкціонованого втручання, традиційно вважалося, що при його вчиненні ставлення винного до будь-яких наслідків, безпосередньо не пов'язаних із інформацією, є необережним. Та навіть якщо уявити, що такі дії цілеспрямовано вчиняються з метою, наприклад, вказаних у ч. 4 ст. 361 КК загибелі людей, завдання їм тілесних ушкоджень, екологічної катастрофи тощо, то вони «безболісно» могли б кваліфікуватися (за відсутності ознак диверсії) за сукупністю, з одного боку, статей 115, 121, 122, 125, 258, 441 КК тощо, а з іншого – частиною 1, 2 або ж, швидше за все, ч. 3 ст. 361 КК.

Стосовно ж посилення відповідальності за несанкціоноване втручання, яке хоча й вчинене в умовах воєнного стану, але без мети заподіяння шкоди державі, то недоречність такого кроку вже була обґрунтована раніше.

Отже, зважаючи на всі вищевикладені аргументи, я дійшов висновку про недоцільність пов'язування посилення відповідальності за несанкціоноване втручання:

– ні зі «створенням небезпеки тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків»;

– ні зі «вчиненням під час дії воєнного стану».

Моє нерозуміння аналізованого законодавчого рішення лише посилюється якщо зважати на те, що, вказавши у ст. 361 КК на відповідні, абсолютно нехарактерні, які не корелюються із характером суспільної небезпеки несанкціонованого втручання кваліфікуючі ознаки, водночас вітчизняні парламентарії «зробили все необхідне» (сподіваюся, що несвідомо) для того, щоб унеможливити диференціацію відповідальності у зв'язку із настанням цілком реальних (принаймні порівняно з попередніми) наслідків несанкціонованого втручання (це ж, до речі, стосується й інших кіберзлочинів).

Мова йде про те, що одним із наслідків ухвалення Закону від 24 березня 2022 р. стало корегування примітки ст. 361 КК, за результатами якого:

– по-перше, було підвищено (зі 100 до 300) виражений у НМДГ показник вказаної у статтях 361–363-1 КК значної шкоди;

– по-друге, і головне, з неї, як свого часу і в добре відомому юристам випадку зі ст. 364 КК, було вилучено існуюче раніше принципово важливо застереження відносно того, що при оцінці «значної шкоди» згаданий майновий еквівалент мав братися до уваги лише тоді, коли така шкода полягала у заподіянні матеріальних збитків. Значущість цього уточнення полягала в тому, що саме воно давало можливість кваліфікувати за ознакою «значної шкоди» і випадки спричинення несанкціонованим втручанням цілком вірогідних наслідків нематеріального характеру: тимчасового зупинення (припинення) роботи або іншого порушення нормального режиму роботи певного підприємства, організації, установи, їх окремих структурних підрозділів; підриву ділової репутації громадянина чи юридичної особи; заподіяння громадянину моральної шкоди внаслідок втрати, незаконного поширення чи витоку інформації, яка є результатом його наукової чи творчої діяльності тощо [2, с. 1115].

Як на мене, помилковість такого кроку, який призвів до суттєвого та нічим невиправданого звуження сфери потенційного застосування ч. 4 ст. 361 КК, є більш ніж очевидною. Тому вважаю, що законодавець якомога швидше повинен:

– або ж **(перший варіант)** «просто» викласти примітку ст. 361 КК в її попередній, існуючій до набрання чинності Законом від 24 березня 2022 р., редакції (оновленого показника НМДГ це не стосується);

– або ж **(другий варіант)**, якщо визнає за доцільне, диференціювати відповідальність за несанкціоноване втручання, що призвело не лише до значної шкоди (наприклад, та ж таки ч. 4 ст. 361 КК) – зміст якої може залишитися незмінним, а й до тяжких наслідків (гіпотетично про них мало б йтися в ч. 5 ст. 361 КК), якими б і могли охоплюватися не лише матеріальні, виражені в НМДГ наслідки (звичайно, вони мають бути вищими, аніж параметри значної шкоди (наприклад, 1000 і більше НМДГ)), а й інші види збитків. При цьому ще раз чітко окреслю свою позицію відносно того, що за вчинення відповідних діянь має бути передбачено істотно м'якше покарання аніж те, що наразі передбачене в ч. 4 та ч. 5 ст. 361 КК.

Крім зазначених вище, М. І. Хавронюк виявив і низку інших, не менш очевидних недоліків технічного характеру, притаманних оновленій редакції ст. 361 КК. Зокрема, вчений зауважує, що:

– замість указівки в ч. 4 на «дії, передбачені ч. 1 або ч. 2 цієї статті», потрібно було вказати на «дії, передбачені ч. 3 цією статті», адже саме по собі несанкціоноване втручання в роботу вказаних систем чи мереж, яке не супроводжується витоком, втратою, підробкою, блокуванням інформації, спотворенням процесу обробки інформації або порушенням встановленого порядку її маршрутизації, не здатне спричинити жодного зі згаданих у відповідній нормі наслідків;

– вказавши у ч. 6 на «дії, передбачені частинами 1–4 цієї статті», парламентарії при цьому «забули» про ч. 5. Через це дії, передбачені ч. 5 ст. 361 КК, навіть якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж, ніби (якщо керуватися буквальним тлумаченням закону) є злочином.

Крім того, М. І. Хавронюк звернув увагу і на тому, що прикінцеві положення Закону від 24 березня 2022 р. вимагають від КМУ розробити та забезпечити введення в дію у місячний строк з дня прийняття цього Закону (тобто до 24 квітня 2022 р.) порядку пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Враховуючи цей факт, науковець констатує, що до часу введення в дію цього порядку (наразі він і досі не затверджений) ст. 361 КК через однозначну бланкетність її диспозицій фактично діяти не може [1].

Загалом погоджуючись із зауваженнями правознавця, все ж дозволю собі припустити, що до трактування аналізованих приписів слід підходити обмежувально

і сприймати їх так, що прийняття згаданого порядку є умовою «розблокування» можливості застосування не всієї, а лише **ч. 6** ст. 361 КК.

Отже, проведене дослідження дало можливість сформулювати авторські рекомендації щодо вирішення найбільш складних правозастосовчих проблем, а також запропонувати зміни до КК, направлені на усунення вад аналізованого Закону. Маю сподівання, що в сукупності це сприятиме досягненню вищої ефективності розглядуваних кримінально-правових приписів.

ЛІТЕРАТУРА

1. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 10-те вид., переробл. та допов. Київ : ВД «Дакор», 2018. 1360 с.

2. Хавронюк М. Втручання в роботу інформаційно-комунікаційних систем: кримінальна відповідальність. URL: https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist/.