– вдосконалення процедури виконання керівником органу прокуратури повноважень слідчого судді;

– оптимізації механізму затримання особи без ухвали слідчого судді задля забезпечення прав такої особи;

– посилення судового контролю над законністю рішень, прийнятими прокурором у порядку статті 615 КПК України.

Таким чином, незважаючи на позитивний досвід удосконалення кримінального процесуального законодавства, окремі питання правової регламентації діяльності органів правопорядку в умовах воєнного стану залишається не до кінця вирішеними і потребують розроблення законодавчих норм з урахуванням необхідності підвищення ефективності кримінального провадження.

Мовчан Роман Олександрович,
професор кафедри конституційного,
міжнародного і кримінального права
Донецького національного університету
імені Василя Стуса, доктор юридичних наук,
професор

ПОСИЛЕННЯ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРЗЛОЧИНИ, УЧИНЕНІ В УМОВАХ ВОЄННОГО СТАНУ: АНАЛІЗ ОБҐРУНТОВАНОСТІ ЗМІН

Перш ніж оголосити про проведення «спєциальной 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 ВРУ 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.).

Результатом ухвалення Закону від 24 березня 2022 р. стало одночасне внесення змін до двох норм КК – статей 361 та 361-1. Зокрема, найбільш серйозніших змін зазнала саме 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 – 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. 615-III КК Італії, ст. 138 КК Нідерландів, ст. 267 КК Польщі);

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 умисного доступу 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 т. ч. 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, як і в ситуації з посиленням відповідальності за мародерство [2], 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 (!!!).

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 тощо.

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.

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.

По-друге, 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, 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 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» 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 вірогідних наслідків нематеріального характеру.

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;

– 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), а й інші види збитків.

Список використаних джерел

1. Хавронюк М. Втручання в роботу інформаційно-комунікаційних систем: кримінальна відповідальність. URL: https://pravo.org.ua/blogs/vtrucha№№ya-v-robotu-i№formatsij№o-komu№ikatsij№yh-system-krymi№al№a-vidpovidal№ist/.

2. Мовчан Р. О. Аналіз законодавчого рішення про посилення кримінальної відповідальності за мародерство. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2022. № 1. С. 281–285.

Мотлях Олександр Іванович,
завідувач наукової лабораторії з проблем
психологічного забезпечення
та психофізіологічних досліджень
Національної академії внутрішніх справ,
доктор юридичних наук, професор

ЗАСТОСУВАННЯ ПОЛІГРАФА В ДОСУДОВОМУ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В УМОВАХ ВОЄННОГО СТАНУ

Розслідування вчинених кримінальних правопорушень було і залишається складним і багатоаспектним процесом, бо передбачає собою застосування компетентними особами вітчизняних правоохоронних органів низки організаційних, технічних, тактичних і процесуальних дій та заходів, які мають між собою бути продуманими, узгодженими й ефективними для своєчасного та якісного забезпечення досудового слідства. Особливого змісту вони набувають в умовах воєнного стану, коли в ході війни України з російським агресором, доводиться й