

2. Війна в Україні може спричинити глобальний голод –ООН. URL: <https://suspilne.media/219201-vijna-v-ukraini-moze-spriciniti-globalnij-golod-oon/>

3. Кримінальне право України: Особлива частина : підруч. / В. Я. Тацій, В. І. Борисов, В. І. Тютюгін та ін. ; за ред. В. Я. Тація, В. І. Борисова, В. І. Тютюгіна. 6-те вид., перероб. і допов. Харків : Право, 2020. 768 с.

*Батургарєєва В. С.,
д.ю.н., професор,
директор Науково-дослідного інституту
вивчення проблем злочинності імені
академіка В. В. Сташица
НАПрН України,*

ЗАКОНОДАВЧІ НОВЕЛИ ЩОДО КРИМІНАЛЬНО-ПРАВОВОГО ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

Перед законодавцем, науковою і практичною спільнотою юристів у зв'язку з воєнними подіями, що мають місце на території нашої держави, постає чимало завдань правового супроводу всебічної протидії агресору та дотримання правопорядку на підконтрольній Україні території, у той час поки дається відсіч Російській Федерації на передовому краї оборони нашої держави.

Як відомо, війна «нового зразка», або «нового покоління», – не лише стратегія ведення війни у її класичному розумінні та битви на полі бою, а це й сучасна військова логістика, створення та підтримка відповідної політичної «атмосфери» ведення війн, робота з настроями великих груп населення, що є соціальною базою для схвалення відповідних дій або, навпаки, своєрідною «п'ятою колоною», що не згодна з воєнно-політичним курсом тієї чи іншої сторони військового протиборства. Інструментом, що опосередковує комунікацію з приводу перелічених «нюансів» війн, звісно ж, є інформаційний простір. Тут ми свідомо не беремо проблему доступності та якості (чистоти) останнього, а лише підкреслимо, що завдяки функціонуванню цього простору стають відомими результати будь-яких діянь, у тому числі протиправних. Більше того, він використовується як плацдарм для вчинення багатьох протиправних діянь. Раніше ми вже відмічали, що протиправні діяння в інформаційному просторі «паразитують» не лише на кіберпросторі як специфічному середовищі, існування якого не уявляється без його

опосередкування інформаційно-комунікаційними мережами та спеціальними пристроями, а й зумовлюють циркуляцію будь-якої інформації, з використанням якої може пов'язуватися вчинення злочину [1, с. 112].

Протягом лютого-квітня 2022 р. до чинного законодавства про кримінальну відповідальність прийнято низку змін і доповнень, а так само введено нові норми. І хоча, на наш погляд, законодавчі новели приймалися в умовах надвеликої емоційності і напруги, що створило, зокрема, колізійну ситуацію у застосуванні їх положень на практиці та породило чимало дискусій у форматі *pro et contra* певних законодавчих підходів, однак головною метою зазначеної новелізації є забезпечення саме кримінально-правового супроводу ефективної протидії збройній агресії та, повторимося, дотримання правопорядку на підконтрольній Україні території.

Як свідчить аналіз вивчених змін і доповнень зазначеного періоду, чимало з них спрямовано на захист інформаційного простору від загроз, які шкодять національній безпеці України в цілому та окремим її складовим, територіальній цілісності та суверенітету, обороноздатності держави, її економіці, праву українського народу на самовизначення, життю та здоров'ю громадян, а так само порушують засади миру та людяності.

В одних випадках убезпечення інформаційних відносин, з безлічі яких зітканий інформаційний простір як такий, є основним завданням захисту кримінально-правовими засобами, в інших – таке завдання вирішується одночасно із захистом правовідносин, що є основним об'єктом складу правопорушення (у таких випадках, напевно, доцільно вести мову про комплексний об'єкт кримінально-правової охорони). Про важливість забезпечення інформаційної безпеки говорить й у Конституції України. Так, згідно зі 17 Основного Закону захист суверенітету і територіальної цілісності України, забезпечення її економічної й інформаційної безпеки є найважливішими функціями держави, справою всього українського народу.

Законом України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24 березня 2022 р. [2] до статей 361 та 361¹ КК (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж) внесено зміни. Зміни до цих статей та їх викладення у новій редакції спрямовано на розв'язання принаймні трьох завдань: 1) приведення термінології, що вживається у зазначених статтях, у відповідність до Закону України «Про електронні комунікації» від 16 груд-

ня 2020 року № 1089-IX [3], а також вимог іншого законодавства України у сфері кібербезпеки; 2) диференціації у ст. 361 КК ступеня відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж з урахуванням наслідків, що настали через це, з відповідним посиленням санкцій за вчинення подібного втручання; 3) доповнення статті новою частиною п'ятою, якою передбачається відповідальність за вчинення аналізованих дій під час дії воєнного стану, що стала рефлексією на збройну агресію проти України з боку РФ.

Оскільки ракурс нашого аналізу сфокусований головним чином на злочинних проявах, що мають місце в умовах воєнного стану, який сьогодні діє на території України, то й міркування насамперед стосуватимуться особливостей запропонованих новел щодо такого періоду. У зв'язку із цим поміркуємо, чи всі діяння, що вчиняються у період часу тривання воєнного стану, доцільно кваліфікувати за ч. 5 ст. 361 КК?

Так, відомо, що комп'ютерне геймерство (захоплення комп'ютерними іграми, як правило, в режимі реального часу з використанням можливостей мережі Інтернету) інколи пов'язано з нечесними діями з боку окремих осіб, особливо коли це захоплення набуває монетизованої форми (продаж гравцем свого ігрового облікового запису або здійснення грошових вкладень у сферу віртуального простору для того, щоб отримати будь-які переваги під час ігрового процесу, купуючи певні віртуальні предмети). Такі нечесні дії можуть бути пов'язані з випадками викрадення у гравців предметів, персонажів гри, блокуванням акаунтів з подальшим вилученням елементів ігрового простору, на придбання яких витрачалися гроші або витрачалось багато часу для створення або набуття можливості використовувати їх. Відповідні дії є ні чим іншим, як несанкціонованим втручанням в роботу електронних комунікаційних мереж, до того ж здатним призвести до витоку, втрати, підробки, спотворення процесу обробки інформації та ін.

Однак, уявляється, що подібні дії менш за все «корелюється» з воєнним станом, а значить, їх кваліфікацію слід визнати, вочевидь, надмірною. Це, з одного боку. З другого боку, коли відбувається несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж об'єктів критичної інфраструктури в обстановці військових подій, і це призводить до серйозних збоїв у забезпечення життєдіяльності суспільства та відсічі ворога в такий час, то, без сумніву, під час кваліфікації вчиненого ця

обтяжуюча обставина має враховуватися. Водночас, цікаво відмітити, що обстановка воєнного стану чомусь не передбачена в інших комп'ютерних злочинах. При такому підході кримінально-правовий захист інформаційного простору має якийсь фрагментарний характер.

Розділ XVI Особливої частини КК України є, так би мовити, класичним прикладом захисту зазначеного простору. Але й в нормах інших розділів Особливої частини КК з'явилися доповнення, що так чи інакше стосуються забезпечення інформаційного простору. Так, наприклад, йдеться про статтю 114², якою Кодекс доповнено відповідним Законом України від 24 березня 2022 р. №2160-IX (зі змінами, внесеними згідно із Законом №2178-IX від 1 квітня 2022 р.) [4]. Предметом зазначеного злочину є певна інформація, що стосується, зокрема, руху різних видів зброї територією України, якщо така інформація не оприлюднювалася у відкритому доступі силовими структурами України або країнами-партнерами. Ця норма є темпоральною, оскільки її дія поширюється тільки на діяння, вчинені в умовах воєнного або надзвичайного стану. При цьому недаремно відповідну статтю введено до розділу I («Злочини проти основ національної безпеки України») Особливої частини КК, адже через порушення певного порядку циркуляції відповідної інформації у надзвичайно складний для країни час, що пов'язаний із необхідністю її оборони від ворога, завдається шкода інтересам держави і суспільства у сфері національної безпеки. Однак поряд із національною безпекою як такою її положення спрямовуються й на захист інформаційної безпеки як частини безпеки національної. Напевно, тут так само має йтися про комплексний об'єкт кримінально-правової охорони, який дозволяє охоплювати всі компоненти національної безпеки, включаючи й безпеку інформаційну.

Неабияку шкоду суспільним відносинам у сфері інформаційного простору завдають кримінальні правопорушення, пов'язані з масованою маніпуляцією певною інформацією, викривленням історичних фактів й подій, внаслідок чого саме в інформаційному просторі (через ЗМІ, різноманітні сучасні комунікатори, що доступні майже всім) має місце потужний вплив як на окремих осіб, так і на великі групи населення. На недопущення такого впливу внаслідок цілеспрямованої інформаційної діяльності спрямована нещодавно прийнята ст. 436¹ КК «Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників». Саме в інформаційному просторі внаслідок зазначених протиправних дій з боку апологетів небезпечних «сентенцій» людина під-

дається свого роду зараженню шкідливими для українського соціуму ідеями й ідеалами. І хоча ця норма розміщена у розділі «Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку» Особливої частини КК, проте негативний вплив протиправних дій стає відчутним в інформаційній сфері, в якій постійно перебуває людина, і за допомогою інструментів саме інформаційного простору.

Подібні міркування стосуються й кримінально-правової новели, передбаченої ст. 111¹ КК («Колабораційна діяльність» (у частині публічного заперечення громадянином України здійснення збройної агресії проти України та публічних закликів щодо всілякого співробітництва з окупаційною владою, а також пропаганди відповідних подій у закладах освіти тощо)). У цьому випадку, як справедливо наголошує О. Кравчук та М. Бондаренко, будь-яка інформаційна діяльність утворює склад злочину, якщо вона відповідає двом ознакам: (1) здійснюється в співпраці з державою-агресором та/або її окупаційною адміністрацією, (2) має відповідне спрямування – на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або на уникнення нею відповідальності за збройну агресію проти України [5].

Список використаних джерел:

1. Батиргареева В. С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право*. № 1(32)/2020. С. 110–119.

2. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 березня 2022 р. № 2149-IX. *Урядовий кур'єр*. 2022. 5 квіт. № 78.

3. Про електронні комунікації: Закон України від 16 грудня 2020 р. № 1089-IX. *Офіційний вісник України*. 2021. 26 січ. № 6. Ст. 306.

4. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24 березня 2022 р. № 2160-IX. *Урядовий кур'єр*. 2022. 28 березн. № 71.

5. Кравчук О., Бондаренко М. Колабораційна діяльність: аналіз нової статті 111–1 Кримінального кодексу України. UTL: <http://hrvector.org/podiyi/22-03-20-mbo>.