РОЗДІЛ 8
КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.3.7
DOI https://doi.org/10.32782/2524-0374/2024-2/77

КРИМІНАЛЬНО-ПРАВОВИЙ АНАЛІЗ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ), ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ

CRIMINAL AND LEGAL ANALYSIS OF UNAUTHORIZED INTERFERENCE IN INFORMATION (AUTOMATED), ELECTRONIC COMMUNICATION, INFORMATION AND COMMUNICATION SYSTEMS AND ELECTRONIC COMMUNICATION NETWORKS

Басараб О.Т., к.ю.н., доцент,
доцент кафедри теорії права та кримінально-процесуальної діяльності
Національна академія Державної прикордонної служби України імені Богдана Хмельницького

Басараб О.К., к.т.н., доцент,
викладач кафедри зв'язку та інформаційних систем
Національна академія Державної прикордонної служби України імені Богдана Хмельницького

У статті проведений кримінально-правовий аналіз кримінального правопорушення, передбаченого ст. 361 Кримінального кодексу України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж».

Автори наголошують, що в умовах вторгнення росії на територію України ця проблема набула особливого значення, оскільки ворог спрямовує численні кібератаки на інформаційні ресурси органів державної влади, військового командування, об'єкти критичної інфраструктури тощо.

Акцентується увага на тому, що необхідність боротьби з кіберзлочинністю в умовах дії воєнного стану в Україні, стрімкий розвиток комп'ютерних технологій та зростання випадків використання їх у злочинних цілях, обумовили необхідність зміни назви первинної редакції досліджуваної статті, корегування її змісту та доповнення її чотирма частинами. Проведено короткий аналіз змін, які мали місце раніше та тих, що пропонуються.

Констатовано, що чинна редакція ст. 361 Кримінального кодексу України містить шість частин, перша з яких є кримінальним правопорушенням, решта відносяться до нетяжких, тяжких та особливо тяжких злочинів.

Проведено характеристику кожного елементу складу досліджуваного кримінального правопорушення. До кваліфікуючих ознак віднесено: вчинення правопорушення повторно, або за попередньою змовою групою осіб; якщо протиправне діяння призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації; якщо протиправне діяння заподіяло значну шкоду чи створило небезпеку тяжких технологічних аварій, або екологічних катастроф, загибелі або масового захворювання населення, чи інших тяжких наслідків; вчинення правопорушення під час дії воєнного стану.

Акцентовано увагу на тому, що ч. 6 ст. 361 Кримінального кодексу України виключає протиправність діяння, якщо воно було здійснено у відповідності до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.

Зроблено висновок про те, що внесені та запропоновані зміни до ст. 361 Кримінального кодексу України є актуальними та такими, що відповідають реаліям сьогодення, особливо в умовах запровадженого воєнного стану в Україні.

Ключові слова: кримінальне правопорушення, несанкціоноване втрачання, воєнний стан, інформаційні системи, комунікаційні системи, електронні комунікаційні мережі, кібератаки, інформаційні ресурси.

The article provides a criminal-legal analysis of the criminal offense defined in Article 361 of the Criminal Code of Ukraine "Unauthorized interference in the operation of information (automated), electronic communication, information and communication systems and electronic communication networks."

Authors emphasize that in the conditions of Russia's invasion of the territory of Ukraine, this problem has acquired special importance, because the enemy directs numerous cyber attacks on the information resources of state authorities, military command, critical infrastructure facilities, etc.

Attention is drawn to the fact that the need to fight cybercrime in the conditions of martial law in Ukraine, the rapid development of computer technologies and the increase in cases of their use for criminal purposes, led to the need to change the name of the primary edition of the article under study, correct its content and supplement it with four parts. A brief analysis of the changes that have taken place before and those that are proposed is carried out.

It was established that the current version of the Article 361 of the Criminal Code of Ukraine contains six parts, the first of which is a criminal offense, the rest refer to minor, serious and especially serious crimes.

The characterization of each element of the composition of the investigated criminal offense was carried out. Qualifying signs include: committing the offense repeatedly, or by a group of persons following a prior conspiracy; if the illegal act led to leakage, loss, forgery, blocking of information, distortion of the information processing process or violation of the established order of its routing; if the illegal act caused significant damage or created a danger of serious technological accidents, or environmental disasters, death or mass illness of the population, or other serious consequences; committing an offense during martial law.

Attention is focused on the fact that Part 6 of Art. 361 of the Criminal Code of Ukraine excludes the illegality of an act if it was carried out in accordance with the procedure for searching and identifying potential vulnerabilities of such systems or networks.

It was concluded that the introduced and proposed changes to Art. 361 of the Criminal Code of Ukraine are relevant and correspond to the realities of today, especially in the conditions of the introduction of martial law in Ukraine.

Key words: criminal offense, unauthorized interference, martial law, information systems, communication systems, electronic communication networks, cyber attacks, information resources.

Вступ. Сьогодні мало хто уявляє своє життя без електронних комунікаційних пристроїв, які дозволяють накопичувати та зберігати величезний обсяг інформації та у найкоротші строки нею обмінюватись. Комп'ютеризація охопила усі сфери суспільного життя.

Водночас, за наявності беззаперечного бенефіту від тотальної цифровізації, існує проблема несанкціонованого втручання у роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж.

Неабиякої актуальності це питання набуло в умовах вторгнення росії на територію України, коли у поєднанні із загарбницькими діями на полі бою, ворог застосовує численні кібератаки на інформаційні ресурси органів державної влади, сектору безпеки і оборони та інші важливі хаби публічної та приватної інформації в Україні.

Так, за даними Державної служби спеціального зв'язку та захисту інформації України, за минулий рік Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA зафіксувала 2 544 кіберінциденти (на 16% більше ніж у 2022 році). Водночас, кількість виявлених кібератак протягом січня-лютого поточного року становить 695 випадків, що вдвічі більше ніж за аналогічний період 2023 року [1].

Тому не випадково, що 09.11.2023 у Верховній Раді України зареєстрували проект Закону № 10242 про внесення змін до Кримінального кодексу України (далі – КК України), яким пропонується встановити кримінальну відповідальність за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах та посилення кримінальної відповідальності за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем в умовах дії воєнного стану [2]. З початку повномасштабного вторгнення, це вже друга зміна, яку пропонується внести до статті 361 кримінального закону, яка викликана необхідністю підвищення ефективності боротьби з кіберзлочинністю під час війни.

Така пристальна увага законотворців до вищезазначеного актуалізує проблему нашого дослідження та спонукає до більш глибшого її аналізу та вивчення на доктринальному рівні.

Аналіз останніх наукових досліджень і публікацій свідчить про те, що питання несанкціонованого втручання у роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж через призму свого предмету дослідження вивчали П. Андрушко, С. Бабанін, А. Білоусов, С. Денис, М. Дмитрук, К. Ісаєв, І. Європіна, Т. Луцький, О. Пасєка, М. Спасибін, А. Тарасюк, М. Щербаковський та інші. Однак, останні зміни до статті 361 КК України та умови запровадженого воєнного стану в Україні, вимагають детального розгляду та дослідження цього складу кримінального правопорушення.

Мета статті. Здійснити кримінально-правовий аналіз кримінального правопорушення, передбаченого ст. 361 КК України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж».

Виклад основного матеріалу. Характеризуючи кримінальне правопорушення, передбачене ст. 361 КК України варто зауважити про високий рівень його латентності, оскільки настання шкідливих наслідків у результаті його вчинення можна спостерігати не відразу, злочинці, зазвичай, працюють дистанційно та застосовують новітню комп'ютерну техніку. Тому невипадково, що протягом 2022 року відносно 1 403 зареєстрованих випадків несанкціонованого втручання у роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, відсоток винесених вироків є не високим [3, с. 305]. Зазначене, на нашу думку, служить ще одним беззаперечним аргументом на користь більш глибокого аналізу досліджуваного кримінального правопорушення.

Варто зауважити, що первинна редакція статті 361 КК України спочатку складалася з двох частин і мала назву «Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», водночас стрімкий розвиток комп'ютерних технологій та зростання випадків використання їх у злочинних цілях, а також необхідність боротьби з кіберзлочинністю в умовах дії воєнного стану в Україні, обумовили необхідність зміни назви статті, корегування її змісту та доповнення чотирма частинами.

Сьогодні, чинна ст. 361 КК України має назву «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» і складається з шести частин. При чому, беручи до уваги положення ст. 12 КК України, тільки протиправні діяння передбачені ч. 1 ст. 361 КК України можуть вважатися кримінальними проступками, решта кваліфікуються як злочини: нетяжкі (ч. 2 ст. 361 КК України); тяжкі (ч. 3 ст. 361 КК України) та особливо тяжкі (ч.ч. 4,5 ст. 361 КК України) [4].

Основним та безпосереднім об'єктом досліджуваного кримінального правопорушення є суспільні відносини у сфері забезпечення роботи інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах»:

– інформаційна (автоматизована) система – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– електронна комунікаційна система – це сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

– інформаційно-комунікаційна система – це сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле [5].

Тлумачення змісту електронної комунікаційної мережі знаходимо у ст. 2 Закону України «Про електронні комунікації», згідно з якою це є комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг [6].

Об'єктивна сторона досліджуваного кримінального правопорушення характеризується дією у вигляді несанкціонованого втручання у роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Несанкціонованим є таке діяння, яке здійснюється без санкції, тобто без дозволу відповідної інстанції, направлене на використання даних, не призначених для вільного доступу [7].

В свою чергу під таким несанкціонованим втручанням слід розуміти будь-які дії, що провадяться з порушенням порядку доступу до інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, установленого відповідно до законодавства [8, с. 831].

Саме такі протиправні дії можуть породжувати настання негативних наслідків, що можуть проявлятися у формі витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації (ч. 3 ст. 361 КК України) [4].

Відповідно до ст. 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах»:

– виток інформації – це результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним або юридичним особам, що не мають права доступу до неї;

– блокування інформації в системі – це дії, внаслідок яких унеможливлюється доступ до інформації в системі [5].

Під втратою інформації розуміють припинення її існування для фізичних, чи юридичних осіб, які мають на неї право власності у повному, чи обмеженому обсязі [8, с. 833].

Викривлення змісту існуючої, або створеної нової інформації, яка за змістом не відповідає дійсності є підробкою інформації, в свою чергу, спотворенням процесу обробки інформації називають зміну перебігу інформації, порядок якого визначений її власником, чи власником автоматизованої системи, чи комп'ютерної мережі, або уповноваженими ними особами [8, с. 833].

Змістом порушення встановленого порядку маршрутизації інформації вважається зміна визначеного відправником інформації адресата, яка передається каналами комунікації, унаслідок чого адресат не отримує інформацію, або крім нього її отримують інші особи, яким вона не призначалася [8, с. 833].

У науковій літературі існують деякі дискусії з приводу виключення законотворцем з ч. 1 ст. 361 КК України переліку наслідків, які можуть наступати в результаті несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, оскільки саме вони та їх причинно-наслідковий зв'язок з протиправним діянням формують об'єктивну сторону досліджуваного кримінального правопорушення [9].

Водночас, аналіз диспозицій статей КК України свідчить про відсутність у змісті деяких прямого вказання на негативні наслідки. Можливо, це обумовлюється самою природою кримінального правопорушення, яке саме по собі є таким суспільно небезпечним та протиправним діянням, що тягне за собою настання різного роду негативних наслідків.

Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж також може завдати значної шкоди, створити небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків (ч. 4 ст. 361 КК України) [4].

Під значною шкодою слід розуміти шкоду, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян [4].

До тяжких наслідків за вчинення кримінального правопорушення, передбаченого ст. 361 КК України законодавець відносить настання тяжких технологічних аварій або екологічних катастроф, загибель або масове захворювання населення тощо.

Чіткого визначення тяжкої технологічної аварії ні у законодавстві, ні у науковій літературі немає. Разом з тим, аналізуючи зміст кожного з цих слів можна припустити, що це є небезпечна подія технологічного характеру, що спричинила ураження, травмування та загрозу життю або здоров'ю населенню. В свою чергу під екологічною катастрофою пропонуємо розуміти велику за масштабами аварію чи іншу подію, яка пов'язана з нанесенням шкоди навколишньому середовищу та призвела до тяжких наслідків.

Суб'єкт досліджуваного кримінального правопорушення загальний: фізична осудна особа, яка досягла шістнадцятирічного віку.

Суб'єктивна сторона характеризується виною у формі прямого, або непрямого умислу.

Кваліфікуючими ознаками кримінального правопорушення, передбаченого ст. 361 КК України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» є:

– вчинення повторно, або за попередньою змовою групою осіб;

– якщо протиправне діяння призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації;

– якщо протиправне діяння заподіяло значну шкоду чи створило небезпеку тяжких технологічних аварій, або екологічних катастроф, загибелі або масового захворювання населення, чи інших тяжких наслідків;

– вчинення під час дії воєнного стану.

При чому, варто зауважити, що така кваліфікуюча ознака як вчинення під час дії воєнного стану є кваліфікуючою лише до ч. ч. 3, 4 ст. 361 КК України.

У контексті розгляду предмету нашого дослідження особливої уваги варта ч. 6 ст. 361 КК України, яка виключає протиправність діяння, передбаченого ч. ч. 1–4 цієї статті, якщо воно було вчинене відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж [4].

Механізм реалізації заходів щодо провадження пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж регламентований Постановою Кабінету Міністрів України від 16.05.2023 № 497 [10].

Висновки. Таким чином, на підставі аналізу складу кримінального правопорушення, передбаченого ст. 361 КК України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», можна дійти висновку про те, що зміст статті повністю відповідає реаліям сьогодення, а внесені та запропоновані новели щодо кримінальної відповідальності за вчинення протиправних дій, передбачених цією статтею в умовах дії воєнного стану, удосконалюють її контент та усувають суттєві прогалини з цього питання.

Представлене дослідження не вичерпує проблему несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем та електронних комунікаційних мереж, а лише доповнює існуючі наукові розробки та обумовлює подальші наші розвідки з цього питання у майбутньому.

ЛІТЕРАТУРА

1. Кіберфронт: українські захисники дають гідну відсіч ворожим атакам. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/kiberfront-ukrayinski-zakhisniki-dayut-gidnu-vidsich-vorozhim-atakam (дата звернення 15.01.2024).

2. Про прийняття за основу проекту Закону України про внесення змін до Кримінального кодексу України щодо встановлення кримінальної відповідальності за несанкціоноване втручання, збут або розповсюдження інформації, що оброблюється в публічних електронних реєстрах, та посилення кримінальної відповідальності під час дії воєнного стану за кримінальні правопорушення у сфері використання інформаційно-комунікаційних систем : Постанова Верховної Ради України від 16.01.2024 № 3551-IX. URL: https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=10242&conv=9 (дата звернення 15.01.2024).

3. С. Бабанін Кваліфікація несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, вчиненого з метою пошкодження об'єктів, які мають важливе

народногосподарське чи оборонне значення. *Міжнародна та національна безпека: теоретичні та прикладні аспекти* : матеріали VII Міжнародної науково-практичної конференції (Дніпро, 17 березня 2023 р.). Дніпро : Вид-во ДДУВС, 2023. С. 304-306.

4. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення 02.02.2024).

5. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення 02.02.2024).

6. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення 02.02.2024).

7. Український мовно-інформаційний фонд НАН України, 2015 – 2024. Словник української мови. Томи 1-14. URL: https://sum20ua.com/Entry/index?wordid=197253&page=1928 (дата звернення 05.02.2024).

8. Науково-практичний коментар Кримінального кодексу України / Д. С. Азаров, В. К. Грищук, А. В. Савченко, В. В. Чернєя. – К.: Юрінком Інтер, 2016. – 1064 с.

9. М. Хавронюк. Втручання в роботу інформаційно-комунікаційних систем: кримінальна відповідальність. URL: https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist/ (дата звернення 15.02.2024).

10. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж : постанова Кабінету Міністрів України від 16.05.2023 № 497. URL:https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text.