обов'язками) закон про кримінальну відповідальність пов'язує наявність у діях особи всіх без виключення складів кримінальних правопорушень, передбачених Розділом VI Особливої частини КК України. І останнє, властивості майна, з якими кримінальний закон пов'язує наявність у діях особи конкретного складу посягання проти власності (речі, майнові права, майнові обов'язки), знаходяться у не у площині визначення кола предметів відповідного кримінального правопорушення (майно, право на майно, дії майнового характеру), а цілковито залежать від ознак об'єктивної сторони того чи іншого складу, тобто характеру суспільно небезпечного діяння, способу його вчинення та природи й обсягу шкоди, спричиненої відповідною протиправною поведінкою об'єкту.

1. Коржанський М. Й. Кваліфікація злочинів проти особи і власності. К. : Юрінком, 1996. 144 с.
2. Дудоров О. О., Письменський Є. О. Кримінальне право (Особлива частина): підручник. Т. 1. Луганськ : «Елтон-2», 2012. 780 с.
3. Олійник П. В. Предмет злочинів проти власності: поняття, види, кримінально-правове значення: монографія. Х. : Право, 2011. 208 с.
4. Тацій В. Я. Об'єкт і предмет злочину в кримінальному праві: монографія. Х. : Право, 2016. 256 с.
5. Музика А. А., Лащук Є. В. Предмет злочину: теоретичні основи пізнання: монографія. К. : Паливода А. В., 2011. 191 с.

УДК 343.3/.7
DOI: 10.31733/17-03-2023-305-307

Сергій БАБАНІН
доцент кафедри
кримінального права та кримінології
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

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

Розпочата російською федерацією війна проти України триває не тільки у реальному просторі, але й у віртуальному – кіберпросторі. З початку 2022 р. Служба безпеки України нейтралізувала понад 4,5 тис. кібератак на Україну. Якщо у 2020 р. було зафіксовано майже 800 кібератак, у 2021 – 1400, то вже минулого року їхня кількість зросла більш як утричі [1].

Наведені дані свідчать про ведення проти України так званої кібервійни. Цей термін достатньо часто використовується на сьогоднішній день у засобах масової інформації, соціальних мережах, у виступах представників органів державної влади [2].

Разом з тим у законодавстві України поняття кібервійни не закріплене. Законом України «Про основні засади забезпечення кібербезпеки України» надається визначення таким поняттям як кібербезпека, кіберзлочин та ін. Так, під кіберзлочином (комп'ютерним злочином), згідно п. 8 ч. 1 цього Закону, мається на увазі суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [3].

При цьому КК України не містить поняття кіберзлочину, а суспільно небезпечні діяння, що вчиняються у кіберпросторі та/або з його використанням, передбачені різними розділами Особливої частини. Основний (але не єдиний) розділ Особливої частини КК України, який містить комп'ютерні злочини – розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», до складу якого входять як злочини, так і

кримінальні проступки [4]. Отже, на сьогодні має місце невідповідність між Законом України «Про основні засади забезпечення кібербезпеки України» та КК України в частині визначення комп'ютерного кримінального правопорушення.

Протягом 2022 р. зареєстровано 3 тис. 415 кримінальних правопорушень, передбачених розділом XVI Особливої частини КК України. З них 1 тис. 403 – несанкціоновані втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України) [5].

Аналіз вироків по кримінальних провадженнях за ст. 361 КК України за період 2022 – початку 2023 років, внесених до Єдиного державного реєстру судових рішень, дозволяє стверджувати про відсутність на сьогоднішній день вироків щодо осіб, які здійснили кібератаки, спрямовані на втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж установ, підприємств та організацій України з метою пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення.

Типовим діянням у вищезазначений період часу, за яке постановлений вирок суду за вчинення кримінального правопорушення, передбаченого ст. 361 КК України, є наступне.

15.11.2022 р. громадянин В. у період часу з 16 год. 41 хв. по 17 год. 11 хв., перебуваючи за адресою: м. Черкаси, вул. Нижня Горова, 70, в умовах воєнного стану, що запроваджений Указом Президента України «Про введення воєнного стану в Україні» від 24.02.2022 р. № 64/2022 та затверджений Верховною Радою України, в подальшому продовжений Указом Президента України від 12.08.2022 р. № 573/2022 до 21.11.2022 р. включно, маючи умисел, спрямований на таємне викрадення чужого майна, переконавшись, що за його діями ніхто не спостерігає та вони є таємними для оточуючих, умисно, таємно, з корисливих мотивів, шляхом несанкціонованого втручання в роботу інформаційних (автоматизованих) систем, викрав грошові кошти, що належать потерпілій С., здійснивши ряд операцій по переказу грошових коштів з банківської картки АТ КБ «ПриватБанк», яка належить потерпілій С. на інші банківські картки [6].

Проте основною метою кібератак, які чиняться представниками російської федерації або за їх підтримки, є пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення. Прикладами таких кібератак є наступні.

15 лютого 2022 р. російські хакери здійснили найпотужнішу в історії України DDoS-атаку, яка, серед іншого, була спрямована на фінансовий сектор (DDoS-атака на 15 банківських сайтів, сайтів з доменом gov.ua, також сайтів Міноборони, Збройних сил та Міністерства з питань реінтеграції тимчасово окупованих територій, що тривала близько 5 годин). 23 лютого 2022 р., перед початком російського вторгнення в Україну, було повторно атаковано низку державних та банківських сайтів [7].

Пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, є обов'язковою ознакою суб'єктивної сторони такого складу злочину як диверсія (ст. 113 КК України).

Предметом диверсії можуть бути, зокрема, об'єкти критичної інфраструктури: тепло- та гідроелектростанції, залізничні та автовокзали, аеропорти, банківські установи, заклади охорони здоров'я тощо.

При цьому склад диверсії за конструкцією є формальним, а отже цей злочин є закінченим з моменту вчинення будь-якого діяння, передбаченого диспозицією ч. 1 ст. 113 КК України.

У разі, якщо особа здійснила несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж для пошкодження діяльності, наприклад, залізничних вокзалів чи електростанцій України, тобто об'єктів, які мають важливе народногосподарське значення, її дії мають ознаки кримінальних правопорушень, передбачених ст.ст. 113 та 361 КК України.

При цьому виникає питання, що має місце у цьому випадку – конкуренція кримінально-правових норм чи множинність кримінальних правопорушень. Сам факт несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж у наведеному прикладі є складовою ознакою діянь, передбачених ст.ст. 113 та 361 КК України. Злочин, передбачений ч. 1 ст. 361 КК України, є закінченим з моменту несанкціонованого втручання в роботу відповідної системи чи мережі, а злочин,

передбачений ч. 1 ст. 113 КК України, є закінченим, якщо відбулась спроба шляхом такого втручання зашкодити діяльності об'єктів, які мають важливе народногосподарське чи оборонне значення.

Таким чином, у цьому випадку має місце ідеальна сукупність кримінальних правопорушень. Якщо особа здійснила несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж з метою пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, такі дії кваліфікуються за відповідними частинами ст.ст. 113 та 361 КК України, а у разі наявності необхідних ознак – і за відповідною частиною ст. 361-1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» КК України.

1. Кібервійна рф проти України: як працюють російські хакери та воюють українські кібервійська. URL: https://thepage.ua/ua/politics/kibervijna-rf-proti-ukrayini-yak-voyuyut-ukrayinski-kibervijska.

2. Федоров про кібервійну з РФ: ми перейшли до «впевненого наступу». URL: https:// www.radiosvoboda.org/a/news-kiberviyna-fedorov/31730708.html.

3. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

4. Кримінальний кодекс України: Закон України від 05.04.2001 р. URL: https://zakon. rada.gov.ua/laws/show/2341-14#Text.

5. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih- dosudovogo-rozsliduvannya-2.

6. Кримінальна справа № 711/607/23. Архів Придніпровського районного суду м. Черкаси. URL: https://reyestr.court.gov.ua/Review/108895380.

7. Кібератаки, артилерія, пропаганда. Загальний огляд вимірів російської агресії. URL: https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi.

УДК 343.32
DOI: 10.31733/17-03-2023-307-309

Лілія БОБРІШОВА
завідувач відділення забезпечення
якості освітньої діяльності
Дніпропетровського державного
університету внутрішніх справ,
доктор філософії в галузі права

НАЦІОНАЛЬНА БЕЗПЕКА ЯК ОБ'ЄКТ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ

Національна безпека – один з фундаментальних елементів існування не тільки держави, але і всієї нації, тому надійний захист цієї соціальної цінності – життєво важлива справа для всього українського народу.

Виняткова важливість національної безпеки знаходить своє відображення і в Конституції України [1]. Зокрема, такі основоположні права людини, як право на конфіденційність приватного життя (ст. 32), право на свободу думки і слова, вільне вираження своїх поглядів і переконань (ст. 34), право на свободу об'єднання у політичні партії та громадські організації для здійснення і захисту своїх прав і свобод та задоволення політичних, економічних, соціальних, культурних та інших інтересів (ст. 36), право на мирні зібрання та мітинги (ст. 39), право на страйк (ст. 44) тощо можуть бути обмежені в інтересах національної безпеки [11, с. 192].

Сутність категорії «національна безпека України» розкривається у Законі України від 21.06.2018 № 2469-VIII «Про національну безпеку України». Так, під нею розуміється захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [8].

З викладеного слідує, що національна безпека передбачає захищеність самого устрою українського суспільства [9, с. 403]. Відтак, посягання на національну безпеку несе високий