Список використаних джерел:

1. Пояснювальна Записка до проекту Закону Верховної Ради України «Про протидію екстремізму». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=49227
2. Бабій А. Ю. Екстремізм як соціальне явище і правова категорія. Кримінальне право та кримінологія. Часопис Київського університету права. 2020/3. С. 296-302.
3. Скулиш Є. Д., Ірха Ю. Б. Екстремізм як одна з головних загроз безпечному існуванню людини, суспільства та держави у XXI ст. Науковий Вісник Національної Академії Внутрішніх Справ, № 1 (98), 2016. С. 19-33.
4. Макс Вебер Про деякі категорії соціології розуміння. URL:http://litopys.org.ua/weber/wbs06.htm

Актуальні секторальні проблеми стійкості критичної інфраструктури

Віталій Павликівський,
д-р юрид .наук, професор, завідувач кафедри права Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: pvictor@i.ua,
ORCID: 0000-0002-1190-9303
Володимир Селевко,
канд. філос. наук, доцент, завідувач відділу аспірантури та докторантури Національного аерокосмічного університету імені М. Є. Жуковського «Харківський авіаційний інститут», м. Харків, Україна
e-mail: v.selevko@khai.edu,
ORCID: 0000-0002-9543-4981

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ РЕЄСТРУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ У БАНКІВСЬКІЙ СИСТЕМІ УКРАЇНИ ТА КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА НЕСАНКЦІОНОВАНЕ ВТРУЧАННЯ В ЙОГО РОБОТУ

Анотація: Розглянута кримінальна подія пов'язана із втручанням у нормальне функціонування оператора телекомунікаційного зв'язку України з боку держави-агресора, а саме у доступі до зв'язку та отримання електронних фінансових послуг через мережу Інтернет. Запропоновано відповідні дії кваліфікувати за Кримінальним кодексом України як диверсія.

Ключові слова: кіберзагроза, кібератака, кіберзахист, банківська інформація, платижна система.

LEGAL ENSURING THE FUNCTIONING OF THE REGISTRY OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS IN THE BANKING SYSTEM OF UKRAINE AND CRIMINAL LIABILITY FOR UNAUTHORIZED INTERFERENCE IN ITS WORK

Abstract: The considered criminal event is related to interference in the normal functioning of the telecommunications operator of Ukraine by the aggressor state, namely in access to communication and receipt of electronic financial services via the Internet. It is proposed to qualify the corresponding actions as sabotage under the Criminal Code of Ukraine.

Keywords: cyber threat, cyber attack, cyber protection, banking information, payment system.

12 грудня 2023 року Україна зазнала одну з найбільш небезпечних кібератак за всі роки незалежності. Незважаючи на те що об'єктом впливу стала Приватне акціонерне товариство «КИЇВСТАР» (далі ПРАТ «КИЇВСТАР») яке надає послуги у забезпеченні безпровідного електронного зв’язку, його наслідки відчула вся країна. Протягом двох днів був відсутній мобільний та інтернет-зв’язок. В результаті таких дій конфіденційна інформація абонентів стала не лише загальнодоступною, але й об’єктом кримінального впливу. Зафіксовано порушення роботи банків, банкоматів і торгових терміналів. Загальні матеріальні збитки уточнюються до цього часу. Як результат, за фактом кібератаки на одного із національних операторів мобільного зв’язку ПРАТ "КИЇВСТАР" Служба безпеки України відкрила кримінальне провадження за вісьмома статтями Кримінального кодексу України. Це, зокрема, ст. 361 КК України (несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж); ст. 361-1 КК України (створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут); ст. 110 КК України (посягання на територіальну цілісність і недоторканність України); ст. 111 КК України (державна зрада); ст. 113 КК України (диверсія); ст. 437 КК України (планування, підготовка, розв'язування та ведення агресивної війни); ст. 438 КК України (порушення законів та звичаїв війни); ст. 255 КК України (створення, керівництво злочинною спільнотою або злочинною організацією, а також участь у ній) [1]. Вказана ідеальна сукупність потребує більш детального аналізу та теоретичного осмислення підходів правоохоронних органів до оцінки вказаних діянь. Враховуючи діяльність держави за останні роки в напрямку діджиталізації органів влади небезпека зазначених діянь в умовах агресії буде тільки підвищуватися. Зокрема це стосується і сфери фінансових та банківських послуг, кровоносної системи будь-якої економіки.

Згідно з Законом України «Про критичну інфраструктуру» та Законом України «Про основні засади забезпечення кібербезпеки України» фінансова та банківська системи України відносяться до І категорія критичності, що вимагає від держави особливої уваги з забезпечення безпеки таких об'єктів, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та протидії кризовим ситуаціям на об'єктах критичної інфраструктури. Таким чином, втручання в банківську інформаційну систему за своїми наслідками може суттєво перевищити збитки, заподіяні ПРАТ «КИЇВСТАР» 12 грудня 2023 року. У зв'язку з цим, в сучасних умовах актуалізується питання правового забезпечення протидії потенційним загрозам та вдосконалення системи кримінально-правового захисту фінансової та банківської системи України, зокрема у сфері електронних комунікацій та захисту інформації.

Одним з напрямків такого вдосконалення в умовах дії воєнного стану виявилося реформування кримінального закону в частині внесення змін до ст. 361 КК України, які стосувалися особливостей несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Незважаючи на те, що у відповідних змінах до закону законодавець врахував особливості потенційних суспільно небезпечних наслідків від несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, важливим залишається питання обґрунтованості кваліфікації за вказаною статтею випадків посягання на інформаційну систему банківських та фінансових установ України в умовах воєнного стану.

Незважаючи на відсутність прямої вказівки в законі на форму вини, аналіз складу кримінального правопорушення, передбаченого ст. 361 КК України дозволяє стверджувати про умисний характер вчинення зазначеного у законі суспільно небезпечного діяння. Про це свідчить і конструкція у виді формального складу відповідного кримінального правопорушення, і наявність такої кваліфікуючої ознаки як вчинення злочину за попередньою змовою групою осіб. В той же час, в диспозиції статті відсутні прямі та непрямі посилання на мотив та мету кримінального правопорушення, що означає ігнорування зазначених обставин законодавцем для визначення підстав криміналізації вказаного суспільно небезпечного діяння.

Зазначимо, що несанкціоноване втручання в роботу інформаційних та комунікаційних систем, особливо під час воєнного стану, не є самоціллю дій злочинців, що і підтверджує випадок з національним оператором "Київстар". Вказані дії виступають лише способом більш небезпечних дій, таких як диверсія, терористичні дії тощо. Врахування зазначених обставин є обов'язковим для правильної кваліфікації та забезпечення законності та повноти застосування кримінального законодавства.

Мета кримінального правопорушення визначає спрямованість суспільно небезпечних дій, а також той уявний результат якого намагається досягти винний. Крім того, визначена мета дозволяє відмежувати злочинні діяння схожі

за характером або такі, що мають тотожні суспільно небезпечні наслідки. Зокрема, саме мета терористичного акту відрізняє останній від схожих за характером та наслідками злочинних дій у вигляді умисного вбивства, умисного знищення або пошкодження чужого майна.

Аналізуючи зміст та характер кібератаки на сервери національного оператора "Київстар" та її наслідків дозволяє стверджувати про те, що несанкціоноване втручання є лише способом досягнення іншої злочинної мети, пов'язаної з ослабленням держави (ст. 113 КК України).

Висновки. Незважаючи на той факт, що диспозиція ст. 361 КК України характеризується лише наявністю умисної форми вини, встановлення мотиву та мети вчинення кримінального правопорушення є обов'язковим для повноти та точності кримінально-правової кваліфікації злочинних дій, пов'язаних з несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

При наявності мети ослаблення держави вказані дії слід кваліфікувати як державну зраду (ст. 111 КК України) або диверсію (ст. 113 КК України).

В той же час, несанкціоноване втручання в роботу інформаційних (автоматизованих) електронних комунікаційних систем як відповідний спосіб диверсії або державної зради вимагає додаткової кваліфікації за ст. 361 КК України.

Список використаних джерел:

1. СБУ відкрила кримінальне провадження за фактом кібератаки на «Київстар» URL.https://ssu.gov.ua/novyny/sbu-vidkryla-kryminalne-provadzhennia-za-faktom-kiberataky-na-kyivstar (дата звернення 04.04.2024)

2. Закон України Про основні засади забезпечення кібербезпеки України URL https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 04.04.2024)

3. Постанова Кабінету міністрів України № 518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури URL https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8

4. Закон України «Про Національний банк України» URL https://zakon.rada.gov.ua/laws/show/679-14#n109