УДК 343.2(477)
DOI: https://doi.org/10.33098/2078-6670.2024.17.29.311-317

ДО ПИТАННЯ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ КІБЕРБЕЗПЕКИ УКРАЇНИ В СУЧАСНИХ УМОВАХ

Чуваков Олег Анатолійович,
доктор юридичних наук, професор,
завідувач кафедри кримінального права, кримінального процесу і криміналістики
Одеського національного університету імені І.І. Мечникова,
Французький бульвар, 24/26, Одеса, Україна, 65058
e-mail: olehchuvakov@gmail.com
ORCID: https://orcid.org/0000-0001-9983-8943

Мета. *З урахуванням існуючих загроз основам національної та військової безпеки України та в умовах геополітичних реалій, що стрімко змінюються, виникає потреба у вдосконаленні існуючої кримінальної політики держави, а також деяких положень кримінального законодавства у сфері належного захисту таких об'єктів кримінально-правової охорони від кібернетичних атак.* ***Методика.*** *Методологічну основу дослідження становить сукупність загальнонаукових принципів і підходів, філософсько-світоглядних і спеціально-наукових* ***методів*** *пізнання соціально-правових процесів і явищ, серед яких: історичний, догматичний, порівняльно-правовий, формально-логічний, системно-структурний, метод моделювання.* ***Результати.*** *У процесі дослідження встановлено необхідність у вдосконаленні низки положень Особливої частини КК України, які дозволять посилити заходи кримінальної репресії щодо антидержавних посягань, що здійснюються шляхом кібератак, а відповідно, переорієнтувати методологічні засади існуючої кримінальної політики нашої держави щодо жорсткості заходів кримінальної репресії з метою локалізації таких антидержавних злочинних проявів у сучасних умовах. Дане положення дозволяє деякою мірою вдосконалити чинне кримінальне законодавство щодо протидії кібернетичним атакам на основи національної та військової безпеки України, а отже, суттєво підвищити ефективність боротьби з ними на сучасному етапі такої охорони об'єктів, що розглядаються.* ***Наукова новизна.*** *У процесі дослідження розроблено науково обґрунтовану концепцію кримінально-правової охорони основ національної та військової безпеки України, яка визначає нові напрями існуючої кримінальної політики держави у даній сфері, а також містить низку пропозицій щодо удосконалення деяких положень чинного кримінального законодавства у сфері охорони кібербезпеки України.* ***Практична значимість.*** *Результати дослідження може бути використано у правотворчій та правозастосовній діяльності під час розслідування злочинів, пов'язаних з використанням сучасних засобів електронних комунікацій, інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів та інших технічних й технологічних засобів та обладнання проти основ національної та військової безпеки України.*

Ключові слова: *кібератака, загроза, кібербезпека, національна безпека, об'єкт, закон, злочин.*

O. Chuvakov
Doctor of Legal Sciences, Professor,
Head of the Department of Criminal Law, Criminal Procedure and Criminalistics
Odesa I.I. Mechnikov National University,
Frantsuzskiy bulvar, 24/26, Odessa, Ukraine, 65058
e-mail: olehchuvakov@gmail.com

ON THE ISSUE OF CRIMINAL LAW PROTECTION OF CYBER SECURITY OF UKRAINE IN MODERN CONDITIONS

Purpose. *Taking into account the existing threats to the foundations of the national and military security of Ukraine and in the conditions of rapidly changing geopolitical realities, there is a need to improve the existing criminal policy of the state, as well as some provisions of criminal legislation in the field of proper protection of such objects of criminal law protection against cyber attacks.* ***Methodology.*** *The methodological basis of the research is a set of general scientific principles and approaches, philosophical-worldview and special-scientific* ***methods*** *of learning socio-legal processes and phenomena, including: historical, dogmatic, comparative-legal, formal-logical, systemic-structural, modeling method.* ***Results.*** *In the process of research, it was established the need to improve a number of provisions of the Special Part of the Criminal Code of Ukraine, which will allow strengthening measures of criminal repression in relation to anti-state offenses carried out through cyber attacks, and, accordingly, to*

reorient the methodological foundations of the existing criminal policy of our state with regard to the severity of criminal repression measures in order to localize such anti-state criminal manifestations in modern conditions. This provision allows to some extent to improve the current criminal legislation on countering cyber attacks on the bases of national and military security of Ukraine, and therefore to significantly increase the effectiveness of combating them at the current stage of such protection of the objects under consideration. ***Originality.*** *In the process of research, a scientifically based concept of criminal law protection of the foundations of national and military security of Ukraine was developed, which defines new directions of the existing criminal policy of the state in this area, and also contains a number of proposals for improving some provisions of the current criminal legislation in the field of cyber security protection of Ukraine.* ***Practical significance.*** *The results of the research can be used in law-making and law-enforcement activities during the investigation of crimes related to the use of modern means of electronic communications, information and communication technologies, software, hardware and other technical and technological means and equipment against the foundations of national and military security of Ukraine.*

Key words: *cyber attack, threat, cyber security, national security, object, law, crime.*

Постановка проблеми. Військове вторгнення Російської Федерації на Україну супроводжується широким застосуванням як сучасної військової техніки, так й активним використанням сучасних засобів електронних комунікацій, інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів та інших технічних й технологічних засобів та обладнання. Така шкідлива діяльність створює загрозу не лише конституційному ладу, суверенітету, територіальній цілісності та недоторканності нашої держави, а й військовій, економічній безпеці, у тому числі й оборонно-промисловому потенціалу загалом. Вчинення в умовах воєнного конфлікту вказаних кримінально протиправних діянь характеризується підвищеним ступенем суспільної небезпеки, оскільки здатні паралізувати, руйнувати, вивести з ладу нормальне функціонування державного апарату, вплинути на нормальне та оперативне управління збройними силами України, вивести з ладу важливі об'єкти критичної інфраструктури тощо.

Аналіз останніх досліджень та публікацій. Подібну проблематику щодо дослідження питань кримінально-правової охорони основ національної та військової безпеки України у своїх наукових працях приділяли увагу Г.В. Андрусів, В.Ф. Антипенко, О.Ф. Бантишев, С.Б. Гавриш, В.О. Глушков, І.В. Діордіца, В.П. Ємельянов, О.М. Костенко, В. А. Ліпкан, М. І. Мельник, Л.В. Мошняга, Ю.В. Нікітін, А.В. Савченко, Є.Д. Скулиш, О.С. Сотула, Є.Л. Стрельцов, В. Я. Тацій, П.Л. Фріс, М.І. Хавронюк, О.В. Шамара, Н.М. Ярмиш, С.С. Яценко та ін.

Постановка завдання. Систематичне застосування противником кібератак істотно знижує рівень захисту простору кібербезпеки нашої держави. У зв'язку з чим виникає невідкладна об'єктивна необхідність адекватної протидії з боку держави таким новим формам антидержавних проявів з використанням засобів сучасної електронно-інформаційної комунікації.

Виклад основного матеріалу дослідження. Згідно з п. 4 ст. 1 Закону України - «Про основні засади забезпечення кібербезпеки України», кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [1].

З метою ефективної протидії подібним загрозам на державному рівні має бути розроблена комплексна стратегія протидії кіберзлочинам як складової системи заходів та засобів, що спрямовані на локалізацію такої злочинності, особливо в умовах існуючого військового конфлікту. Основні напрями подібної діяльності держави в аналізованій сфері мають визначати зміст її оновленої, переосмисленої політики у сфері протидії кіберзлочинності. Однак, вітчизняна доктрина кримінального права поки не розробила комплексну, єдину, узгоджену концепцію кримінально-правової політики, яка спрямована на протидію кібератакам, особливо в умовах воєнного конфлікту. Ця обставина пояснюється й тим, що досі не розроблено, зокрема, політичні засади відповідних напрямів державної діяльності у сфері охорони українського кіберпростору, як власне, й способи захисту суспільних відносин від подібних злочинних посягань. Вказана концепція має стати фундаментальним правовим підґрунтям щодо інших напрямів такої політики, серед яких особливе місце посідають: кримінально-правова політика у сфері охорони основ національної та військової безпеки України, у сфері забезпечення миру, безпеки людства та міжнародного правопорядку тощо.

Вважаємо, що ефективність та результативність кримінально-правової політики у сфері забезпечення кібербезпеки держави визначається не стільки вибором того чи іншого концептуального вектора її розвитку, скільки рівнем якості змісту та ступенем продуктивності реалізації нормативних приписів чинного вітчизняного кримінального законодавства, яке з урахуванням існуючих загроз та політичної обстановки в Україні потребує кардинальних змін. Саме в цей період видається очевидним, що чинна система кримінально-правової охорони кібербезпеки потребує свого переосмислення, а відповідно, й певних змін, що дозволило б адекватним чином протидіяти існуючим потенційним загрозам у цій важливій сфері життєдіяльності нашої держави. Концепція протидії кіберзлочинам має бути частиною єдиної сучасної кримінально-правової політики України, яка б відповідала викликам сьогодення та враховувала злочинні загрози іншим об’єктам кримінально-правової охорони в умовах воєнного конфлікту, а саме національній, громадській безпеці тощо. Необхідно розробити систему новітніх засобів протидії вказаним видам злочинності із використанням електронно-інформаційних комунікацій, інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних та технологічних засобів й обладнання, які мають відповідати принципово новому рівню такого захисту, який був би здатним нейтралізувати такі посягання як на сучасному етапі захисту нашої державності, так і в майбутньому.

Необхідно зазначити, що досі не розроблені необхідні принципи, критерії, що дозволяють наочно визначити межі кола суспільно небезпечних зазіхань, які повною мірою завдають або можуть завдати шкоди основам кібербезпеки України. Нами пропонуються певні зміни до певних норм чинного Кримінального кодексу України, які здатні підвищити ефективність протидії кіберзлочинам та можуть стати частиною тих законодавчих змін, яких потребує чинний Кримінальний кодекс України для вирішення викликів сьогодення.

Так, у чинному Кримінальному кодексі України всі суспільно небезпечні діяння, які вчиняються за допомогою засобів електронних комунікацій, інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних та технологічних засобів і обладнання зосереджені законодавцем у Розділі XVI Особливої частини – «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж

електрозв'язку». Кримінальні правопорушення вказаного розділу (згідно з їх безпосередньою спрямованістю) загалом носять абстрактний, загальний й певною мірою невизначений характер, що у сучасних умовах (особливо за умов військового конфлікту) ставить під сумнів їх оперативну ефективність. У зв'язку з цим нами пропонується розглядати такі дії не відокремлено/абстрактно, а залежно від безпосередньої спрямованості їх вчинення, але з урахуванням тієї їхньої специфіки та особливостей, які передбачені зазначеним «спеціальним» розділом чинного Кримінального кодексу України. Тобто йдеться про необхідність наявності спеціальних складів кіберзлочинів, які можуть зазіхати на ті чи інші об'єкти кримінально-правової охорони, залежно від конкретного спрямування такого кримінального правопорушення. У таких кримінальних правопорушеннях досягнення поставленої мети можливе лише у разі його вчинення за допомогою відповідної кібератаки, шляхом застосування засобів електронних комунікацій, інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних та технологічних засобів й обладнання.

У теперішній час найбільш актуальними напрямами для подібних атак (з урахуванням сучасних викликів) є, насамперед, посягання на основи національної безпеки України (суверенітет, конституційний лад, територіальну цілісність та недоторканність, обороноздатність держави), а також на відносини у сфері забезпечення миру, безпеки людства та міжнародного правопорядку.

Щодо посягань на основи національної безпеки України, то певних удосконалень потребують деякі норми цього розділу Особливої частини Кримінального кодексу України.

Так, диспозиції складів злочинів, передбачених статтями 109 та 110 КК України («Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади» та «Посягання на територіальну цілісність і недоторканність України»), слід було б доповнити деякими кваліфікованими ознаками їх вчинення, а саме – *«шляхом застосування кібератак»*.

Як свідчить міжнародна практика, а саме, згідно з подіями, що мали місце в Єгипті, Тунісі, Венесуелі, Туреччині, Лівії, Іраку, Сирії та інших державах, антидержавні злочинні дії, спрямовані на повалення існуючих режимів, а саме організація державних переворотів (у тому числі й успішних) найчастіше здійснювалися шляхом широкого застосування сучасних засобів електронної комунікації.

На прикладі антидержавних проявів у зазначених державах, широке застосування засобів інформаційно-комунікаційних технологій можуть бути спрямовані як на ініціювання, так і на координацію всіляких акцій протесту, переважно молоді та студентів, які згодом повільно переростають у відкриті бунти незадоволених існуючим режимом. Причому «ідеологічно підковані» молоді люди легко можуть об'єднуватися в різні правозахисні, етнічні, релігійні, а по суті – екстремістські організації. З метою сприяння наростаючим протестам та дезорганізації правоохоронних заходів у протидії їм, можуть бути здійснені синхронні кібератаки на різні урядові сервери. Подібні злочинні акти тільки вселяють екстремістам почуття вседозволеності та безкарності, що сприяє поширенню таких антиурядових виступів, які продовжують контролюватись їх організаторами, в тому числі і за допомогою засобів електронних комунікацій. Такі прояви поступово набувають все більш організованого і спланованого характеру і здатні перерости в масові заворушення, основною метою яких найчастіше є насильницьке захоплення державної влади та повалення існуючого легітимного конституційного ладу.

Як не дивно, стандартною (основною), у кожному конкретному випадку причиною таких заворушень, які переростали в антиконституційну зміну правлячого режиму, було невдоволення мас утиском прав і свобод громадян, авторитаризм та корумпованість їхніх лідерів тощо. Проте, особливе місце серед таких виступів займає невдоволення протестувальників підсумками чергових виборів (референдумів) у державі, які натовпом визнавалися неконституційними. Як правило, таким подіям може передувати добре спланована серія кібератак як на сервери окремих виборчих дільниць, так і на сервери центральної виборчої комісії, чим паралізується нормальна їх робота, а, відповідно, утруднюється процес об'єктивного підрахунку голосів. Ситуація, що складається, безумовно, не може не бути використана екстремістами в досягненні своїх злочинних антидержавних цілей.

Не можна не відзначити також, що особлива роль у підбурюванні до таких масових виступів їх організаторами відводилася до широкого використання популярних соціальних мереж.

У цьому зв'язку, як нам уявляється, доцільно статті 109 та 110 чинного КК України доповнити відповідними кваліфікованими ознаками, спрямованими на протидію кібератакам, що посягають на основи національної безпеки України. У контексті існуючої геополітичної дійсності такі злочини не зовсім відображають їх сучасну політико-правову сутність, тобто в подібній редакції ознаки таких складів не відповідають в повному обсязі тим загрозам та викликам, які існують в об'єктивній дійсності. У тому числі беручи до уваги ту обставину яких масштабів набула загроза широкого застосування подібних кібератак.

Отже, пропонується ч. 3 ст. 109 КК України – «Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади» доповнити таким змістом:

3. *Дії, передбачені частиною другою цієї статті, вчинені особою, яка є представником влади, або повторно, або організованою групою, або за допомогою засобів масової інформації, або вчинені шляхом здійснення кібератак,-*

Відповідно, ч. 2 ст. 110 КК України – «Посягання на територіальну цілісність та недоторканність України» пропонується доповнити аналогічним змістом:

2. *Ті самі дії, якщо вони вчинені особою, яка є представником влади, або повторно, або за попередньою змовою групою осіб, або поєднані з розпалюванням національної чи релігійної ворожнечі, або вчинені шляхом здійснення кібератак, -*

Як уже зазначалося, в сучасних умовах комп'ютерні технології, інтернет та різні телекомунікаційні системи займають особливе місце у житті громадян, підприємств, установ та організацій, нормальне функціонування та життєдіяльність яких безпосередньо залежать від таких систем. У зв'язку з цим посягання на нормальну роботу відповідної інфраструктури, може спричинити за собою порушення життєдіяльності цілих населених пунктів, телефонних систем, систем електро-водо- газо- постачання, транспорту, атомної енергетики тощо. Отже, використання засобів електронних комунікацій, інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних та технологічних засобів й обладнання в таких цілях може завдати істотної шкоди не тільки підприємствам, установам або окремим громадянам, а й економічної безпеки держави.

Дана обставина свідчить про необхідність криміналізації подібних злочинних проявів - кібернетичних атак. У зв'язку з чим, диспозицію статті 113 КК України

пропонується доповнити новою формою здійснення такого злочину - «вчинення кібернетичних атак».

У зв'язку з наданою аргументацією нами пропонується наступна оновлена редакція ст. 113 КК України:

«Вчинення з метою ослаблення держави вибухів, підпалів, кібернетичних атак або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень або іншої шкоди їхньому здоров'ю, на руйнування чи пошкодження об'єктів, що мають важливе народногосподарське чи оборонне значення, а також здійснення з цією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій».

Однак, застосування подібних технологій в сучасних умовах і, особливо з урахуванням геополітичної обстановки, що стрімко змінюється у світі, здатне завдавати істотних збитків не тільки основам національної безпеки держави, а й миру і безпеки людства. Йдеться про можливість застосування засобів електронних комунікацій, інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних та технологічних засобів й обладнання, в тому числі і з метою встановлення контролю/управління над найсучаснішими, передовими видами озброєнь, які, як правило, повністю автоматизовані і найчастіше їх нормальне та ефективне функціонування забезпечується відповідним програмним забезпеченням спеціального (воєнного) призначення.

Встановлення несанкціонованого контролю за такими видами озброєнь (наприклад, потенційного противника) дає можливість ініціаторам таких злочинних кібервтручань завуальованим чином спровокувати військовий конфлікт між державами певного регіону. При цьому держава-ініціатор таких кібератак, маючи на меті отримання бажаних геополітичних результатів, набуває можливості здійснювати таку діяльність «тіньовим» чином, у тому числі, можливо, й безкарно. У зв'язку з цим пропонуємо внести зміни до нормативних приписів, закріплених у Розділі XX Особливої частини КК України – «Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку». Зокрема, пропонується ч. 2 ст. 439 «Застосування зброї масового знищення» доповнити таким змістом:

2. *Застосування зброї масового знищення, вчинене шляхом кібернетичної атаки* –

Отже, пропонуємо наступну редакцію вказаної статті:

Стаття 439. Застосування зброї масового знищення

1. Застосування зброї масового знищення, забороненої міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, -

2. Застосування зброї масового знищення, вчинене шляхом кібернетичної атаки –

3. Діяння, передбачені частиною першою або іншою цієї статті, якщо вони спричинили загибель людей або інші тяжкі наслідки, -

Висновки. Отже, запропоновані нами законодавчі зміни дозволять посилити заходи кримінально-правової репресії щодо антидержавних посягань на основи кібербезпеки України.

Подібного роду вдосконалення деяких положень кримінального законодавства, сприятимуть подальшому процесу уніфікації та диференціації чинного Кримінального кодексу України щодо протидії протиправним кібернетичним посяганням на основи

національної та військової безпеки України, а, отже, істотно підвищити ефективність протидії ним на сучасному етапі кримінально-правової охорони вказаних об'єктів.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10. 2017 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст.403.

References

1. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine dated No. 2163-VIII (2017, October 5). *Vidomosti Verkhovnoi Rady* 2017. 45, 403. (in Ukrainian)

Стаття: надійшла до редакції 26.03.2024
прийнята до друку 11.04.2024
The article: is received 26.03.2024
is accepted 11.04.2024

Бібліографія: Чуваков О. А. До питання кримінально-правової охорони кібербезпеки України в сучасних умовах. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Журнал. Серія Право*. Івано-Франківськ: Редакційно-видавничий відділ Університету Короля Данила, 2024. Вип. 17 (29). С. 311-317. DOI: https://doi.org/10.33098/2078-6670.2024.17.29.317-317