DOI https://doi.org/10.30525/978-9934-26-409-2-24

FOREIGN EXPERIENCE OF CRIMINAL LIABILITY FOR UNAUTHORIZED INTERFERENCE WITH INFORMATION (AUTOMATED), ELECTRONIC, COMMUNICATION, INFORMATION AND COMMUNICATION SYSTEMS, ELECTRONIC COMMUNICATION NETWORKS

ЗАРУБІЖНИЙ ДОСВІД КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА НЕСАНКЦІАНОВАНЕ ВТРУЧАННЯ В РОБОТУ ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ), ЕЛЕКТРОННИХ, КОМУНІКАЦІЙНИХ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ, ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ

Dryzhakova D. Y.
third level applicant, Postgraduate Student at the Department of Criminal Law and Policy and Criminal Law Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

Дрижакова Д. Ю.
здобувач третього рівня, аспірант кафедри кримінально-правової політики та кримінального права Київський національний університет імені Тараса Шевченка
м. Київ, Україна

З метою ґрунтовного дослідження кримінальної відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних, комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, визначення шляхів подальшого розвитку, удосконалення вітчизняного законодавства в цій сфері потрібно розглянути законотворчу діяльність іноземних держав і вивчити кримінально-правові норми деяких зарубіжних країн, що встановлюють відповідальність за подібний злочин, а також відповідні положення міжнародного права.

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.

Ключовим різностороннім міжнародним документом з кібербезпеки є Конвенція про кіберзлочинність (Будапештська конвенція), прийнята Радою Європи у 2001 році та ратифікована Законом України від 7 вересня 2005 року № 2824-IV[1]. У цій Конвенції наведена

класифікація комп'ютерних злочинів і рекомендації органам влади держав щодо боротьби з цими злочинами.

Для реалізації кримінально-правових норм в процесі протидії кіберзлочинності законодавцям країн-членів ЄС необхідно було внести зміни до кримінально-процесуального законодавства та профільних законів, які регламентують оперативно-розшукову діяльність і діяльність у сфері електронних комунікацій у частині, що стосується процесуальних прав органів дізнання та слідства, фіксації доказів в електронній формі, проведення обшуків і вилучення ЕОМ, систем та мереж, а також інформації, яку вони містять [2].

Серед універсальних міжнародно-правових документів, окрім згаданої Конвенції, вирізняємо Довідник ООН із запобігання і контролю злочинності, пов'язаної з комп'ютерами, 1995 рік; Конвенцію ООН проти транснаціональної організованої злочинності, 2000 рік. Одним із перших міжнародних документів у боротьбі з кіберзлочинністю є «Мінімальний список» правопорушень у цій сфері, прийнятий Європейським комітетом з проблем злочинності Ради Європи у 1990 році, який передбачав наступні злочини: комп'ютерне шахрайство, комп'ютерний підлог, пошкодження комп'ютерної інформації чи програм, комп'ютерний саботаж, несанкціонований доступ до комп'ютерних систем, несанкціоноване перехоплення інформації, несанкціоноване копіювання захищених комп'ютерних програм, незаконне виготовлення топографічних копій. Згодом ця класифікація злочинних посягань була скорегована Конвенцією 2001 року. З метою протидії міжнародній кіберзлочинності, а також для координації діяльності правоохоронних органів країн світу такі злочини класифікуються за кодифікатором міжнародної кримінальної поліції Генерального Секретаріату Інтерполу, який з 1991 року інтегровано в автоматизовану систему пошуку, і сьогодні він доступний підрозділам Національних центральних бюро Інтерполу більшості країн світу, зокрема, й НЦБ Інтерполу МВС України[3].

Ще одним важливим документом у забезпеченні кібербезпеки на міжнародному рівні є Директива про безпеку мереж та інформаційних систем (The Directive on security of network and information systems (NIS Directive), ухвалена Європейським парламентом у 2016 році.

Зважаючи на важливість процесів у кіберпросторі та зростання кіберзагроз у цій сфері, світові держави розробляють свої стратегії кібербезпеки та відповідне національне законодавство.

Законодавство про кримінальну відповідальність за несанкціонований доступ до комп'ютерних мереж в різних країнах світу суттєво відрізняється. Не у всіх державах воно в належній мірі адаптоване до постійно зростаючих потреб посилення кримінально-правової охорони правовідносин, пов'язаних з використанням комп'ютерних технологій та інформації. Вивчення накопиченого в інших країнах законодавчого досвіду дозволить виробити пропозиції щодо вдосконалення норм Кримінального кодексу України в частині забезпечення безпеки використання комп'ютерної інформації.

Аналіз суб'єктивних ознак складів несанкціонованого доступу, закріплених у КК зарубіжних держав, показує наступне. По відношенню до суб'єктивної сторони можна говорити, що більшості вивчених КК мало місце вказівка на умисну форму вини. Таким чином, можна говорити про практично повну уніфікацію кримінального законодавства у цьому плані. Необережна форма вини зустрічається набагато рідше в кваліфікованих складах несанкціонованого доступу, причому альтернативно з умисною формою вини (КК Бельгії).

Що ж стосується суб'єкта досліджуваного злочину, то таким в більшості випадків є фізична осудна особа. А от відносно віку притягнення до кримінальної відповідальності за несанкціонований доступ до комп'ютерної інформації зарубіжні законодавці також не досягли єдності, що пов'язано з різними підходами у встановленні віку кримінальної відповідальності в цілому. Так, з 14 років передбачена відповідальність у Кореї, Австралії; з 15 років – у Норвегії, Швеції, Данії, Туреччини, штаті Техас; з 16 років – у КНР, Голландії; з 15 років – у Польщі. При цьому в деяких державах передбачена можливість залучення до відповідальності і в більш ранньому віці за умови вчинення злочину умисно. Так, в КК Швейцарії цей вік встановлений з 7 до 15 років, з 10 до 14 років – в КК Австралії, з 11 до 15 років – у Туреччині, з 12 до 16 років – у Голландії. Крім того, в КК Бельгії, Австралії, Франції, Данії, Норвегії встановлена і відповідальність юридичних осіб [4].

Аналізуючи кваліфікуючі ознаки несанкціонованого доступу, закріплені в КК зарубіжних держав, можна сказати наступне. Ряд КК (Австрія, Австралія, КНР, Швейцарія) містять тільки основний склад несанкціонованого доступу, що не має кваліфікованих видів. У той же час в інших КК міститься низка кваліфікуючих ознак, серед яких найчастіше зустрічаються наступні: несанкціонований доступ з наміром здійснити облудну операцію (з метою отримати незаконний

дохід), з використанням службового становища (перевищенням повноважень), заподіяв певної шкоди, що спричинив зміну або знищення даних, з метою вилучення (копіювання) даних. Серед інших кваліфікуючих ознак можна вказати такі, як несанкціонований доступ, вчинений повторно, організованою групою, за наказом, що спричинив погіршення функціонування комп'ютерної системи. Таким чином, можна зробити висновок, що й кваліфіковані види несанкціонованого доступу вельми різноманітні.

Для повної характеристики несанкціонованого доступу має важливе значення і аналіз санкцій, які передбачають покарання за злочин з основним складом у КК зарубіжних держав. У 92% санкції є альтернативними і відносно визначеними. Слід зазначити, що значна частина КК передбачає в санкції за даний злочин два види покарання максимальну кількість покарань – три, і тільки в КК Австралії вказаний один вид покарання. Причому в переважній більшості (за винятком КК КНР) в якості одного з покарань передбачений штраф, причому в КК Бельгії, Австрії і штату Техас вказані розміри штрафу. В якості альтернативи штрафу частіше за інших передбачено тюремне ув'язнення. Причому відносно цього виду покарання слід зазначити наступне. У деяких КК законодавці передбачили термін позбавлення волі до 6 місяців (Австрія, Голландія, Данія, Норвегія) або до 1 року (Бельгія, Франція). Таким чином, законодавці даних країн віднесли несанкціонований доступ до злочинів, які не представляють великої суспільної небезпеки. В інших КК законодавці встановили термін позбавлення волі до 3 років (КНР, ФРН, Туреччина, Польща), тобто в цих державах суспільна небезпека даного злочину підвищена, і його можна відносити до категорії менш тяжких.

Проведений аналіз КК зарубіжних держав виявив деякі особливості, які заслуговують уваги. По-перше, це відсутність вказівки на настання можливих наслідків, що дозволяє відносити в багатьох державах даний склад до формальних. По-друге, це вказівка на умисну форму вини.

Таким чином, незважаючи на те, що несанкціонований доступ знайшов законодавче закріплення в кримінальному законодавстві багатьох зарубіжних держав, відсутній уніфікований підхід до опису ознак складу даного злочину. Відсутність одноманітного підходу до криміналізації несанкціонованого доступу не сприяє ефективній протидії даного злочину.

Література:

1. Конвенція про кіберзлочинність (Будапештська конвенція). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
2. Присяжнюк М.М. Організаційно-правові основи забезпечення кібербезпеки. Київ : Видавництво Ліра-К, 2023. С. 194–195.
3. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. УДК 341.01. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf
4. Criminal Code of Germany. URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

DOI https://doi.org/10.30525/978-9934-26-409-2-25

CURRENT ISSUES OF CRIMINAL AND LEGAL MEASURES FOR COMBATING CYBERCRIME

АКТУАЛЬНІ ПИТАННЯ КРИМІНАЛЬНО-ПРАВОВИХ ЗАСОБІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Zakharchenko A. Y.
master's student
Educational and Scientific Institute of Information Security and Strategic Communications
of the National Academy of the Security Service of Ukraine
Kyiv, Ukraine

Захарченко А. Є.
студентка магістратури
Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій
Національної академії Служби безпеки України
м. Київ, Україна

Kamenskyi D. V.
Doctor of Law,
Professor at the Department of Criminal Law
National Academy of the Security Service of Ukraine
Kyiv, Ukraine

Каменський Д. В.
доктор юридичних наук,
професор кафедри кримінального права
Національна академія Служби безпеки України
м. Київ, Україна

Кіберзлочинність – це одна з основних проблем XXI ст., вирішення якої потребує розробки та застосування кримінально-правових засобів ефективної протидії цьому явищу [1, с. 129]. Додатково актуалізує