Інтернет-ресурсі з використанням підроблених імен користувача, профілів або облікових записів, у ст. 209 КК Іспанії – серйозні образи, вчинені з використанням реклами; у ч. 2 ст. 373, ч. 2 ст. 376, ч. 2 ст. 378 КК Казахстану – публічні образи з використанням засобів масової інформації чи мереж телекомунікацій.

Мають місце випадки криміналізації образи в межах кваліфікованих чи особливо кваліфікованих складів окремих кримінальних правопорушень. Наприклад, у ст. 332, 333 КК Грузії образа особистої гідності потерпілого є кваліфікуючою ознакою зловживання службовими повноваженнями та перевищення службових повноважень.

Наведене свідчить про те, що правова охорона представників влади у законодавстві зарубіжних держав здійснюється зокрема за допомогою норм КК. Водночас криміналізація відповідних діянь відбувається по-різному: мають місце відмінності у різновидах образи, що пов'язані як з способом, місцем їх вчинення, категорією потерпілих осіб, кількістю та різновидами заборонних кримінально-правових норм, які містять відповідні підстави кримінальної відповідальності, поєднанні образи з іншими кримінально протиправними діяннями, а також місцем цього діяння в системі ознак кримінального правопорушення тощо.

Біленчук Петро Дмитрович,
професор кафедри кримінального права
і процесу юридичного факультету
Національного авіаційного університету,
кандидат юридичних наук, доцент;
Лихова Софія Яківна,
завідувач кафедри кримінального права
і процесу юридичного факультету
Національного авіаційного університету,
доктор юридичних наук, професор;
Малій Микола Іванович,
директор правничої компанії
ТОВ «АЮР-КОНСАЛТИНГ»

ШЛЯХИ РЕФОРМУВАННЯ КРИМІНАЛЬНОЇ КІБЕРПОЛІЦІЇ НА СУЧАСНОМУ ЕТАПІ ЦИВІЛІЗАЦІЙНОГО РОЗВИТКУ

Сьогодні варто зазначити, що 23.11.2001 р. історичною подією для цивілізованого світу стало підписання важливого правничого документу в Будапешті «Конвенції про кіберзлочинність» державами-членами Ради Європи та іншими державами, які усвідомлювали глибокі зміни, спричинені розвитком електронної ери і переходом всіх

сфер життя на електронні (цифрові) технології, конвергенцію і глобалізацію комп'ютерних мереж.

Зазначимо, що наша держава долучилась до даної визначної міжнародної ініціативи 7.09.2005 р., ратифікувавши Законом України «Про ратифікацію Конвенції про кіберзлочинність» «Конвенцію про кіберзлочинність» та, згідно статті 9 Конституції України такі основоположні норми «…є частиною національного законодавства України».

Беручи до уваги чільні правові положення «Конвенції про кіберзлочинність» та враховуючи значне зростання динаміки кіберзлочинності в світі наказом МВС України № 322 від 27.07. 2009 р. було створено відділ боротьби з кіберзлочинністю у складі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми з дев'ятьма співробітниками в штаті.

Відомо, що згідно Наказу Національної поліції України від 07.11.2015 р. № 10 «Про затвердження Штату Департаменту кіберполіції Національної поліції України» передбачено залучення в штат чотирьохсот фахівців з кібербезпеки. Згідно Наказу Національної поліції України від 10.11.2015 р. № 85 було затверджено «Положення про Департамент кіберполіції Національної поліції України».

Аналізуючи стан практичної діяльності Департаменту кіберполіції Національної поліції України з 2015 року до початку 2022 року нами встановлено відсутність чіткої налагодженої організаційно-правової, інформаційно-комунікаційної та процесуальної взаємодії між Головним управлінням та регіональними відділеннями Національної поліції на всій території України в ході реагування на кіберінциденти. Семирічний консолідований системний асиметричний аналіз діяльності кіберполіції України свідчить про відсутність дієвої реєстрації кіберінцидентів, а також неналежне правове забезпечення запобігання та протидії кіберзлочинів відповідно до засадничих положень чільного законодавства України.

Проведений нами асиметричний аналіз слідчої, експерно-криміналістичної, судової та правозахисної практики за сім років дозволив виявити та підтвердити юридичний факт вчинення першого в Україні космічного кіберзлочину, який нещодавно вже розглянутий в українському суді [1].

Даний перший космічний кіберзлочин був вчинений на території і космічному просторі України, а також на територіях та космічному просторі семи держав світу (на чотирьох континентах – Американському, Африканському, Євразійському та Європейському) з допомогою використання потужних інструментів міжнародних систем супутникового зв'язку та державних і приватних наземних станцій електрозв'язку ще в жовтні 2018 року [2].

Варто особливо звернути увагу на те, що офіційні письмові, електронні та особисті звернення жертви кіберінциденту до державних установ України та правоохоронних органів (до Уповноваженого Верховної Ради України з прав людини, до Голови Верховного Суду України, до Голови Апеляційного господарського суду та інших місцевих апеляційних та касаційних інстанцій України, до Генерального прокурора України, до голови Ради національної безпеки і оборони України, до Міністра внутрішніх справ України, до керівництва Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, до голови Департаменту у сфері захисту персональних даних, до керівництва Департаменту Кіберполіції Національної поліції України, до керівництва Департаменту кіберполіції Київського управління кіберполіції Національної поліції України, до десяти районних управлінь поліції міста Києва Головного управління Національної поліції України до Департаменту у сфері захисту персональних даних) жодних результатів не дали. Ці звернення жертви кіберінциденту згідно статті 1, 3, 5 Конституції України та іншого чільного законодавства не зобов'язали виконати норми закону щодо реакції державних правоохоронних органів хоча б спроби розпочати розслідування даного кіберзлочину. Аналіз фактичних документів реагування правоохоронних органів на кіберінцидент свідчить, що дані установи порушують чільне законодавство та надають практично типові шаблонні відписки. Цікавим є те, що дані правоохоронні органи фактично заяви про кіберінцидент не реєструють в Єдиному реєстрі досудового розслідування. Слід зазначити, що якщо в поодиноких випадках реєструють такі заяви про кіберінцидент, то їх слідчі не розслідують, а справи необгрунтовано та безпідставно закривають. Це свідчить про юридичні доказові факти скоєння кримінальних правопорушень даними посадовими особами.

Здійснений нами системний аналіз матеріалів судових засідань свідчить, що жодна правнича служба кібербезпеки шести держав світу і України, а також їх безпекових телекомунікаційних установ (операторів космічних телекомунікацій, операторів магістральних телекомунікаційних мереж супутникового зв'язку, операторів наземних телекомунікаційних служб) фактично не зреагували на даний кіберінцидент. Це фактично свідчить, що державні органи семи країн світу не зацікавилися злочинною дією електронних зловмисників, оскільки не виявили, не задокументували і не здійснили відповідні правничі, технологічні, безпекові заходи щодо протидії цим кіберінцидентам (космічним кібератакам, кіберзагрозам, кіберзлочинам) здійсненим як в наземному, так і в космічному електронному кіберпросторі [3].

Важливо акцентувати увагу на тому, що даний трафік кібератак здійснювався посекундно понад 24 години підряд (в період з

14.10.2018 р. по 18.10.2018 р.). Цікавим є і те, що ці наземні і космічні електронні кібератаки здійснювалися з інтервалом інколи до секунди, а в більшості випадків тривалістю від однієї, двох, трьох, чотирьох та більше секунд. Також, слід зазначити, що за одну секунду сьогодні технологічно можливо передавати 1440 кілобайт інформації. Очевидно, що за двадцять чотири години цей показник складає значно більшу кількість переданих важливих відомостей, даних тощо.

Відомо, що зовсім недавно, а саме в ніч з 13 на 14.01.2022 р. було здійснено неймовірно масштабну та блискавичну злочинну кракерську атаку на надзвичайно важливі урядові сайти України. Причому, на головних сторінках атакованих сайтів було розміщено повідомлення провокаційного характеру [4].

Варто також зауважити, що дана кібератака була здійснена на сімдесят державних сайтів України. Дана кібератака була здійснена саме після вдалого запуску українського супутника «Січ 2-30» і виведеного на орбіту Землі [5]. Фактично до переліку атакованих сайтів потрапили установи критичної інфраструктури України, а саме: Кабінету міністрів України, Міністерства закордонних справ, загальноукраїнського порталу Дії, Державної казначейської служби, Державної служби України з надзвичайних ситуацій, Міністерства освіти і науки, Міністерства енергетики та інші.

Це свідчить про те, що такі кібератаки здійснені з наземних та космічних сфер фактично порушують конституційні права людини, суспільства, держави, а також є особливо небезпечними для гарантування миру, безпеки людства та міжнародного правопорядку.

Вважаємо, що сьогодні українським державним та правоохоронним органам необхідно консолідувати свої зусилля з метою по запобігання, протидії, розслідуванню вчинених наземних та космічних кіберзлочинів. З цією метою необхідно: по-перше, забезпечити обов'язкову та миттєву реєстрацію кіберзлочинів в Єдиному реєстрі досудових розслідувань згідно положень чільного законодавства; по-друге, налагодити тісну співпрацю з відповідними безпековими міжнародними органами світу (ООН, ОБСЄ, ЮНЕСКО, ФАТФ, МПА, Інтерпол, Європол) і державними установами (Великої Британії- Мі5, Мі-6; США – АНБ, ЦРУ, ФБР; України – РНБО та інших країн), а також з освітніми та науковими установами (університетами, інститутами, академіями, коледжами, безпековими науково-дослідними інститутами). Для цього необхідно розробити і реалізувати не тільки в освіті, науці, але і на практиці стратегічні кроки щодо прийняття відповідних безпекових управлінських стратегічних та тактичних рішень; по-третє, забезпечити якісне та блискавичне запобігання, протидію, розслідування не тільки надзвичайно небезпечних кіберзлочинів, але і всіх наявних кіберзлочинів без винятку [6; 7; 8].

Список використаних джерел

1. Сопілко І.М., Лихова С.Я., Біленчук П.Д. Космічний кіберзлочин як загроза національній безпеці України. Матеріали XV Міжнародної науково-технічної конференції «АВІА-2021». Київ: НАУ, 2021. URL: http://conference.nau.edu.ua/index.php/AVIA/AVIA2021/paper/view/8017/6667.
2. Лихова С.Я., Біленчук П.Д. Космічні і наземні кіберзагрози третього тисячоліття: засоби пізнання, доказування, розслідування // Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». 2021. Т. 2, № 59. С. 9–17.
3. Біленчук П.Д., Лихова С.Я., Малій М.І. Космічні кіберзагрози в третьому тисячолітті: наукове і правове пізнання. 50 років академічної науки на Закарпатті: матеріали міжнародної конференції (м. Ужгород, 24-25 травня 2021 року). Укладач: А.М. Завілопуло, д.ф.-м.н. Інститут електронної фізики НАН України. м. Ужгород: Видавництво «ФОП Сабов А.М.», 2021. 288 с. С. 283–286.
4. Кіберполіція, СБУ та Держспецзв'язку встановлюють причетних до кібератак на сайти державних структур URL: https://cyberpolice.gov.ua/news/kiberpolicziya-sbu-ta-derzhspeczzvyazku-vstanovlyuyut-prychetnyx-do-kiberatak-na-sajty-derzhavnyx-struktur-1630/.
5. Біленчук П.Д., Малій М.І., Сватюк Н.І. Правове і наукове забезпечення міжзоряних польотів: електронний космічний всесвіт / П.Д. Біленчук, М.І Малій, Сватюк Н.І. // Юридичний Вісник України, 2022. № 4. С. 12–13.
6. Біленчук П.Д., Малій М.І. Карне електронне право Європи й України: порівняльний аналіз Ч.1 / П.Д. Біленчук, М.І. Малій // Юридичний Вісник України, 2021. № 8. С. 12–13. https://lexinform.com.ua/dumka-eksperta/karne-elektronne-pravo-yevropy-j-ukrayiny-porivnyalnyj-analiz/.
7. Біленчук П.Д., Малій М.І. Карне електронне право Європи й України: порівняльний аналіз Ч.2 / П.Д. Біленчук, М.І. Малій//Юридичний Вісник України, 2021.-№9. С. 11. https://lexinform.com.ua/dumka-eksperta/karne-elektronne-pravo-yevropy-j-ukrayiny-porivnyalnyj-analiz-chastyna-2/
8. Біленчук П.Д., Малій М.І. Карне електронне право Європи й України: порівняльний аналіз Ч.3 / П.Д. Біленчук, М.І. Малій // Юридичний Вісник України, 2021. № 10. С. 14–15. https://lexinform.com.ua/dumka-eksperta/karne-elektronne-pravo-yevropy-j-ukrayiny-porivnyalnyj-analiz-chastyna-3.