випадку наслідком цього може бути засудження невинної особи за тяжкий злочин.

У висновку слід зазначити, що існування подібної норми є виправданим, адже проблема є нагальною для нашої держави. Водночас, законодавець геть безвідповідально поставився до юридичного закріплення ст. 255[1], у вигляді численних неточностей та необґрунтованої конкуренції з іншими нормами, що майже унеможливлює її практичне застосування. Також, на нашу думку, фрази на кшталт «будь-які дії особи», «здійснює інший вплив», «іншим особистим якостям чи можливостям» взагалі не повинні використовуватись у Кримінальному кодексі України.

Література

1. Кримінальний кодекс України: Закон України від 23.08.2021 № 1292-IX. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

2. Кримінально-виконавчий кодекс України: Закон України від 03.07.2020 № 720-IX. URL: https://zakon.rada.gov.ua/laws/show/1129-15#Text

УДК 343.851(043.2)

Рубанов О.І., здобувач вищої освіти
першого (бакалаврського) рівня,
Київський університет права НАН України, м. Київ, Україна
Науковий керівник: Сисоєва В.П., к.ю.н.

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Головною ознакою кіберзлочинності є її глобальна розповсюдженість. Сьогодні кібератаки можуть зупиняти діяльність не тільки окремих об’єктів господарської діяльності, але й державних органів, таким чином жодна країна світу не може бути повністю захищеною від кіберзлочинів. Часто джерелом ймовірної кіберзагрози є не хакер або об’єднання хакерів, але й окремі терористичні, злочинні угруповання, підрозділи спеціальних служб різних держав тощо.

З прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» було вкрай необхідним, вироблення єдиного понятійного апарату, як першого кроку на шляху до правової боротьби з кіберзлочинністю. Але до визначення поняття кіберпростір, кіберзлочин, кіберзлочинності і кібербезпеки потрібно підходити ретельно не тільки тому, що в результаті неправильної законодавчого формулювання можна знівелювати всю раніше проведену роботу, але й у зв’язку з ймовірною неможливістю застосувати норму на практиці. Враховуючи відмінні

ознаки цього виду злочинності, законодавство про протидію та запобігання таких порушень повинно прийматися з урахуванням міжнародних норм та напрацювань. Заходи запобігання кіберзлочинності, що закінчуються по лінії кордону країни, будуть безрезультатними, без урахування досвіду інших держав, а також без міжнародного співробітництва, в сучасних умовах не представляється можливим досягнення кібербезпеки жодної навіть найрозвинутішої країни [1, с. 155]. Цей Закон враховує міжнародні стандарти протидії кіберзлочинності, а також визначає основні поняття, пов'язані з нею.

Відповідно до Конвенції про кіберзлочинність, яка є частиною українського законодавства з 11.10.2005 р., кіберзлочини умовно поділяються на чотири види. До першого виду належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. До цього виду кіберзлочинів можна віднести всі кримінальні правопорушення, спрямовані проти комп'ютерних систем і даних. До другого виду кіберзлочинів належать правопорушення, пов'язані з комп'ютерами. Такі правопорушення характеризуються умисним діянням, що призводить до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, не маючи на це права, економічних переваг для себе чи іншої особи. Третій вид кіберзлочинів охоплює правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі. Четвертим видом є умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог вітчизняного та міжнародного законодавства. Існують також інші класифікації кіберзлочинів, проте запропонована конвенцією є найбільш популярною [2]. Відповідно до цього, слід зазначити, що протидія кіберзлочинності має містити заходи реагування та запобігання кожній окремій групі кіберзлочинів.

Сьогодні таку діяльність в Україні, головним чином, забезпечують спеціальні підрозділи правоохоронних органів, наприклад, Департамент кіберполіції у складі Національної поліції України. Такі підрозділи займаються розслідуванням значних, суттєвих порушень кібербезпеки. А дрібні шахрайства у кіберпросторі залишаються підслідними підрозділам кримінальної поліції. Крім спеціальних підрозділів, безпеку в інтернет-мережі також повинні підтримувати інтернет-провайдери та власники інформаційних систем. Зокрема, керівники служб безпеки банків, інших критичних в інформаційному відношенні установ перш за все повинні зважено підходити до питання доцільності використання інтернет-послуг.

Для ефективної протидії віртуальним злочинцям необхідна багаторівнева інституційна система кібербезпеки, яка захищала б і простих громадян, і державні інститути. Система кібербезпеки включає в себе різноманітні компоненти, у тому числі підвищення рівня цифрової грамотності населення, сприяння в просуванні індивідуальних засобів захисту особистої інформації, механізми з протидії та профілактики кіберзагроз. Таким може стати Департамент кіберполіції Національної поліції України [3].

Підводячи підсумки, слід зауважити, що загроза кіберзлочинності є міжнародною проблемою і тому протидія їй не може обмежуватися кордонами якоїсь країни. Відповідно до Конвенції про кіберзлочинність, існує декілька груп кіберзлочинів і тільки системна протидія кожному із цих видів кримінальних правопорушень матиме позитивний ефект в майбутньому. Основними шляхами протидії кіберзлочинності в Україні в умовах сучасності слід визначити: забезпечення багаторівневого технічного захисту інформації; підготовка кваліфікованих кадрів у цій галузі; удосконалення нормативно-правового забезпечення заходів реагування на кіберзлочини тощо.

Література

1. Таволжанський О.В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право*. 2018. № 6(18). С. 154-163.

2. Нікулеско Д. Кібербезпека: вразливі моменти. *Юридична газета online*. URL: https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html

3. Піголь Р.С. Актуальні шляхи запобігання злочинності у сфері комп'ютерних технологій. Науковий блог Національного університету «Острозька академія». URL: https://naub.oa.edu.ua/2017/актуальні-шляхи-запобігання-злочин/