Дорошенко Анастасія Григорівна,
здобувач ступеня вищої освіти бакалавра факультету міжнародної торгівлі та права Державного торговельно-економічного університету;
Кудінова Дар'я Дмитрівна,
здобувач ступеня вищої освіти бакалавра факультету міжнародної торгівлі та права Державного торговельно-економічного університету
Науковий керівник:
Шведова Г. Л., доцент кафедри правового забезпечення безпеки бізнесу Державного торговельно-економічного університету, кандидат юридичних наук, доцент

КРИМІНАЛЬНО-ПРАВОВА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ: АКТУАЛЬНІ ПИТАННЯ

У наш час стрімкий розвиток інформаційних технологій не тільки надає нам багато можливостей, а й породжує нові загрози – одною з них є кіберзлочинність. Це явище стало серйозним випробуванням для правової системи України і потребує не тільки оновлення законодавства, а й удосконалення механізмів його реалізації на практиці.

Кіберзлочинність, як явище – не просто сукупність правопорушень, а ціла система відповідних суспільно небезпечних діянь, які ставлять пвд загрозу державу та її інформаційну безпеку. В Україні, як і в більшості країн світу, відзначається швидке зростання кількості кібератак. Одним із найвідоміших випадків став вірус Petya, що в 2017 році спричинив зупинку роботи державних установ, банків та великих компаній. За інформацією Служби безпеки України, протягом 2024 року було знешкоджено близько 4000 кібератак, спрямованих на органи влади та об'єкти критичної інфраструктури. [1]

Можна погодитися з думкою А. В. Микитчика, що кіберзлочинність має низку специфічних рис: високотехнологічність, латентність, транскордонність і тісний

зв'язок з організованою злочинністю. Значну частину таких кримінальних правопорушень вчиняють професійні хакерські групи, які діють у міжнародних мережах і мають на меті отримання матеріальної вигоди. Особливо небезпечними формами є кібертероризм і кіберекстремізм, які можуть становити реальну загрозу життю людей та інформаційній безпеці держави. [2]

Кібертероризмом є злочинна діяльність, здійснена з використанням інформаційно-комунікаційних технологій**,** з метою дестабілізації суспільства або впливу на органи влади**.** До кібертерористичних дій відносяться: атаки на критичну інфраструктуру (енергетичні системи, транспорт, зв'язок), злам державних або військових інформаційних систем, поширення дезінформації з метою залякування населення.

Кіберекстремізм є використанням Інтернету чи цифрових технологій для пропаганди радикальних ідей**,** розпалювання ворожнечі, закликів до насильницьких дій з політичних, релігійних чи ідеологічних мотивів. Прикладами є: поширення в соцмережах екстремістських матеріалів, створення онлайн-спільнот для вербування учасників радикальних рухів, використання цифрових платформ для організації незаконних акцій тощо.

В Україні кримінальна відповідальність за кіберзлочини передбачена розділом 16 КК України. Санкції цих норм містять покарання від штрафу до позбавлення волі на строк від 3 до 15 років, залежно від тяжкості злочину завданих збитків та кваліфікуючих обставин. [3]

Щодо протидії з цій загрозі, справедливою є думка А. В. Микитчика про те, що: «Перш за все слід відійти від вирішення проблеми запобігання кіберзлочинності шляхом подолання існуючих тенденцій і перейти до активної розробки інформаційної безпеки на випередження. Також він зазначає, що необхідним є об'єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян». [2]

Підтримуючи цю позицію зазначимо, що ефективна протидія кіберзлочинності можлива лише за умови консолідації зусиль державних інституцій, правоохоронних органів, бізнес-сектору, наукового середовища та громадянського суспільства. Основними напрямами такої діяльності мають бути розвиток

професійного потенціалу фахівців у галузі кібербезпеки, розширення міжнародного співробітництва й обміну досвідом, а також утвердження правової культури безпечного та відповідального використання цифрових технологій.

Список використаних джерел

1. З початку року СБУ нейтралізувала майже 4 тис. кібератак на органи влади та критичну інфраструктуру України. Служба безпеки України. URL: https://ssu.gov.ua/novyny/460-kiberatak-i-20-khakerskykh-uhrupovan-neitralizuvala-sbu-z-pochatku-roku

2. Микитчик А.В. Заходи запобігання кіберзлочинності в Україні. Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку. Харків, 2019. URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf

3. Кримінальний кодекс України від 05.04.2001 р. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

4. Никончук Н.С., Маслова О.О. Кіберзлочинність в Україні: виклики сучасності. URL: http://www.lsej.org.ua/9_2021/51.pdf

Зінченко Ірина Олександрівна,
здобувач ступеня вищої освіти бакалавра навчально-наукового інституту права та психології Національної академії внутрішніх справ
Науковий керівник:
Резнік Ю. С., старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук

ВІКТИМОЛОГІЧНИЙ ПОРТРЕТ ТА МОДЕЛІ ПОВЕДІНКИ ЖЕРТВ КІБЕРЗЛОЧИНІВ

«Жертва злочину є не просто об’єктом, а активним учасником кримінальної ситуації, чия поведінка, свідома чи несвідома, може або сприяти, або перешкоджати вчиненню