Б. М. Орловський
д.ю.н., доц.

КРИМІНОЛОГІЧНИЙ АНАЛІЗ СТРУКТУРИ КІБЕРЗЛОЧИННОСТІ

Кіберзлочинність є одним із сучасних видів злочинності, який має тенденцію до постійного розширення по мірі комп'ютеризації економічних відносин у суспільстві та розвитку інформаційних технологій. Сучасні банківська та торгівельна сфери активно застосовують обслуговування клієнтів із використанням мережі Інтернет, що визначає можливість перехоплення персональних даних їх клієнтів злочинцями та подальшого вчинення кримінальних правопорушень з використанням отриманих даних. У зв'язку з викладеним актуальним є аналіз сучасної кримінологічної структури кіберзлочинності та порівняння її змісту із наявними нормами Кримінального кодексу (далі – КК) України, що отримали відповідні зміни та доповнення за рахунок приєднання України до Конвенції про кіберзлочинність [2; 3, с. 157].

За своєю структурою кіберзлочини можна поділити на наступні групи: 1) спрямовані на порушення конфіденційності, цілісності і доступності даних і комп'ютерних систем. Зазначена група охоплює злам бази даних на сервері відповідного сайту та отримання конфіденційної інформації про користувачів даного ресурсу або системи (наприклад, отримання логінів та паролів банківських клієнтів, отримання персональних даних осіб, що зареєстровані користувачами певного сайту – ПІБ, місця проживання, телефонів тощо); 2) втручання у роботу комп'ютерної системи шляхом умисного створення серйозних перешкод її функціонуванню. Зазначена група охоплює різноманітні DOS-атаки на ключову інформаційну інфраструктуру системи з наміром зробити комп'ютерні ресурси недоступними користувачам, коли одночасно відбувається декілька тисяч запитів до системи, в результаті чого система виходить із ладу; 3) поширення вірусного програмного забезпечення, що виводить із ладу інтернет-ресурс, систему або окремий комп'ютер. Така група кіберзлочинів передбачає розроблення умисно шкідливих вірусних програм, які поширюються

у мережі Інтернет під виглядом встановлення безоплатних корисних програмних компонентів або ж у вигляді пропозицій перейти на вірусний сайт у електронних поштових листах, що надсилають користувачам. Зазначені вірусні програми здійснюють знищення програмного забезпечення користувача або знову ж таки намагаються отримати персональні дані про користувача; 4) пов'язані із порушенням авторських та суміжних прав, а саме незаконним копіюванням змісту сайтів або окремих частин сайтів, розміщенням однотипних сайтів без погодженням із їх власником; 5) пов'язані із створенням шахрайських сайтів, які окрім дублювання змісту офіційних сайтів, надають можливість зчитати персональні дані особи (наприклад логін і пароль користувача банку, данні банківської картки для розрахунків тощо). Отримуючи такі дані злочинці у подальшому здійснюють списання грошових коштів із банківського рахунку особи через відповідні інтернет-операції. Зазначена група злочинів у міжнародному правовому полі має відповідні назви, наприклад: інтернет-фішинг – створення підроблених сторінок, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів тощо; скімінг – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера), встановленого у банкоматі; смс-фішинг – надсилання через смс фіктивної інформації про блокування певного платіжного інструменту (наприклад, банківської картки) з пропозицією ввести свої персональні дані для розблокування такого платіжного інструменту; вішинг – отримання персональних даних щодо реквізитів платіжного інструменту (наприклад банківської картки) за допомогою телефонних дзвінків від імені банку або певної платіжної системи тощо; 6) поширення в інтернет-мережах протиправного контенту, що містить пропаганду фонових явищ (наприклад, наркоманії, продажу наркотиків, проституції, расової та релігійної нетерпимості тощо).

Якщо ми звернемо увагу на структуру кримінальних правопорушень, що забезпечують протидію кіберзлочинності у Розділі XVI КК України, то можемо побачити, що вони охоплюють перелічену різновиди кіберзлочинності, зокрема ст. 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних

систем, електронних комунікаційних мереж» охоплює першу група описаних кіберзлочинів; ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку» охоплює другу групу описаних кіберзлочинів; ст. 361-1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» охоплює третю групу описаних кіберзлочинів [1]. В той же час у цих статтях відсутня конкретизація об'єктивної сторони відповідних різновидів кіберзлочинності, а також до них не потрапили питання кваліфікації певних різновидів кіберзлочинності, пов'язані із використанням банківських платіжних інструментів, які охоплюються ст. 200 КК України щодо незаконних дій з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима тощо.

Висновки. Кримінальний кодекс України потребує конкретизації та подальшого розвитку системи кримінальних правопорушень у сфері кіберзлочинності, що закріплені у Розділі XVI, зокрема більш детального розкриття об'єктивної сторони таких складів кримінальних правопорушень.

Список використаної літератури

1. Кримінальний кодекс України : зі змінами та доповненнями станом на 01.09.2021 (офіційний текст). Київ : Видавництво «Паливода А.В.», 2021. 264 с.
2. Конвенція про кіберзлочинність : ратифікована Законом України № 2824-IV від 07.09.2005р. *Офіційний вісник України*. 2007. № 65. Стор. 107. Ст. 2535.
3. Кравцова О.М. Сучасний стан і напрямки протидії кіберзлочинності в Україні. *Вісник Кримінологічної асоціації України*. 2018. № 19. С. 155–166.