

РОЗДІЛ 2.
КРИМІНАЛЬНО-ПРАВОВІ, ПРОЦЕСУАЛЬНІ
ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ
КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 343.9:[004.738.5:316.613.434]

КАЗНАЧЕСЬКА Дар'я Володимирівна,

кандидат юридичних наук, доцент,

доцент кафедри кримінального права і кримінології факультету № 1

Харківського національного університету внутрішніх справ;

ДОРОШ Анастасія Олександрівна,

курсантка 4 курсу факультету № 2

Харківського національного університету внутрішніх справ

ВІКТИМНІСТЬ У КІБЕРПРОСТОРИ

Розвиток сучасного суспільства в світовому масштабі завжди визначається глобальними викликами сучасності. Серед них особливе місце займають виклики, пов'язані з розвитком і впровадженням цифрових технологій в різні сфери життєдіяльності людини і сучасного соціуму, які породжують не тільки позитивні зміни, але і певні загрози для його членів. Поступ людства до інформаційного суспільства, діджиталізація економіки, культури та й побутового життя передбачає здійснення частини звичних практик у цифровому просторі (кіберпросторі): спілкування із близьким і віддаленим соціальним оточенням, а відтак набуття соціального досвіду із відповідним засвоєнням соціальних норм, цінностей і розбудовою стосунків; пошук інформації для забезпечення предметної діяльності, ведення поточних справ і забезпечення повсякденних потреб (фінансово-економічні, соціокультурні, громадсько-політичні аспекти людської діяльності також все більше набувають «оцифрованого» характеру).

На сьогодні людство переживає швидкий перехід різних сфер життєдіяльності до мережі «Інтернет», як то обіг безготівкових грошових коштів, неконтрольовані державою фінансові взаєморозрахунки у віртуальній (цифровий) валюті, кібершахрайство, кібербулінг тощо. За даними проведених досліджень Інтернетом регулярно користуються близька 71% українців і ця кількість постійно зростає [1].

Погоджуємось із думкою, що у масовій свідомості вже давно констатується розрив між технологіями, зокрема й інформаційними, та гуманітарною сферою, соціальним розвитком, і при цьому спостерігається неспіврозмірне, загрозливе випередження темпів розвитку перших [2, с.137].

Разом з тим зазначену динаміку злочинності загострило і введення в Україні з березня 2020 року особливих карантинних умов, викликаних пандемією COVID-19. Зазначений режим обмежив права громадян, перш за все, на свободу пересування. Тому багато хто з них був змушений залишатися в місцях проживання (перебування) та виконувати вимоги суворої самоізоляції. Вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем.

Можна спостерігати тенденцію до стрімкого зростання комп'ютерної злочинності, в першу чергу, фінансових шахрайств з використанням соціальної інженерії- вішинг, а також фішінга- жертвами яких ставали, в основному, клієнти банків. Активно використовувалася експлуатація теми протидії COVID-19 під виглядом шкідливих розсилок, посилилось залучення нових учасників до діяльності злочинних спільнот, упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків. За даними звіту

Європолу щодо оцінки зареєстрованих злочинів режим карантину особливо позначився на зростанні кіберзлочинності, торгівлі контрафактними та неякісними товарами, а також різних видів шахрайства і схем, пов'язаних з організованою злочинністю [3].

Аналіз статистичних даних, а також наукових публікацій у нашій державі також підтверджують зазначену тенденцію. Так, наприклад, *«у вересні 2021 року працівники кіберполіції Херсонщини виявили протиправну діяльність трьох чоловіків, які видаючи себе за працівників служби безпеки банку випитували у громадян реквізити їхніх банківських карток та відомості для доступу до онлайн-банкінгу. Надалі через додаток онлайн-банкінгу фігуранти переказували гроші з карток потерпілих на підконтрольний рахунок»* [4].

В той же час *«у вересні 2021 року співробітники управління протидії кіберзлочинам м. Києва викрили правопорушника, який купував на анонімних форумах у мережі DarkNet бази авторизаційних даних користувачів різних програм лояльності відомих платіжних систем та компаній. За допомогою власноруч написаних скриптів із застосуванням автоматизованої системи, перевіряв їх відповідність до існуючих облікових записів громадян. Надалі - авторизувався в особистих кабінетах користувачів та привласнював гроші з їхніх бонусних рахунків. За попередніми підрахунками, у такий спосіб чоловік ошукав понад сотню осіб»* [5].

Можна зазначити, що такі особливості цифровізації суспільства, як 1) змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту, а також 2) стрімка віртуалізація реальності, 3) інформаційна соціалізація, 4) зниження емоційного інтелекту, породжують певні загрози суспільству і державі в цілому.

Саме для запобігання та протидії кіберзлочинності у 2001 р. у Будапешті була прийнята Конвенція про кіберзлочинність, яка була ратифікована Верховною Радою України із застереженнями і заявами Законом № 2824-IV від 07.09.2005 р. Крім того, в Україні прийнято Закон «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 р. Однак, швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя. Саме для виконання цих завдань у серпні 2021 року Указом Президента України № 447/2021 затверджено Стратегію кібербезпеки України.

Наведені вище аргументи, на нашу думку, свідчать про необхідність та доцільність не тільки вивчення кіберзлочинності, а й «корпусу» її жертв.

На сьогодні немає єдиної думки щодо визначення та предмету віктимології. Однак можна цілком погодитись із думкою О.М. Джужи, «...що особливе значення для кримінологічної науки має розвиток кримінологічної віктимології як комплексної міждисциплінарної галузі, що досліджує проблему жертви злочину з позиції кримінального, кримінально-процесуального, кримінально-виконавчого права, криміналістики та кримінології» [6, с. 134].

З іншого боку, як справедливо зауважують О.М. Литвинов та Ю.В. Орлов, розмаїття ситуацій, що виникають під час вчинення злочинів, з очевидністю свідчить про необхідність вивчення жертви злочину. В її структурі віктимологічно значущою може виявитись будь-яка з безлічі людських властивостей: від анатомічних та біологічних до психологічних та соціальних. І однозначно не можна сказати, які дії потерпілого здатні спровокувати вчинення злочину. Тому дійсно особу, яка вчиняє злочин, потерпілого та особливості ситуації вчинення злочину варто розглядати як дві частини одного цілого - системи механізму злочинної поведінки [2, с. 164-165].

На нашу думку, проблема вивчення жертв протиправних посягань, що вчиняються у кіберпросторі, є однією із фундаментальних для сучасної науки з певних причин.

По-перше, на сьогодні взагалі недостатньо досліджень та даних щодо зазначеної категорії потерпілих, також треба наголосити, що за даними ООН близька 80 % потерпілих взагалі не звертаються до правоохоронних органів [8, с. 25].

По-друге, розвиток цифрових технологій та їх стрімка розповсюдженість серед населення значно підвищує кількість потерпілих від зазначеної категорії злочинних посягань.

По-третє, вивчення жертв протиправних посягань, що вчиняються у кіберпросторі буде сприяти виявленню масштабів цього явища та допоможе розробити заходи профілактики останньому.

В рамках дослідження ми вирішили провести анкетування молоді, а саме курсантів та студентів нашого університету у віці від 18 до 22 років у кількості 290 респондентів щодо їх досвіду у мережі Інтернет, а також випадків індивідуальної віктимізації у цій сфері. Із загальної кількості опитаних 65% склали особи чоловічої статі, 35% - жіночої.

Так, на питання «Як часто Ви користуєтесь мережею Інтернет?» - 99% респондентів відповіли, що підключаються до Інтернету кожен день. А 91% - щоденно користуються соціальними мережами.

Щодо випадків передачі персональних даних, а саме реквізитів документів, адрес, номерів телефонів або адрес електронної пошти стверджено відповіли 87% опитаних (див. табл. 1.).

Таблиця 1

Структура передачі конфіденційної інформації в мережі Інтернет

Ресурс	% від загальної кількості респондентів
Державні послуги	65 %
Веб банкінг	79 %
Онлайн магазини	53 %
Запис до медзакладів	41 %
Сайти перевізників (наприклад, Укрзалізниця)	67 %
Реєстрація на різних тематичних порталах	38 %
Сайти оголошень (наприклад, OLX)	27 %

На запитання «Чи траплялись по відношенню до Вас неправомірні діяння у мережі Інтернет?» - 72 % респондентів відповіли, що так. Після проведеного опитування було виокремлено основні кібер загрози, або можна сказати різні форми віктимізуючих діянь (див. табл. 2.).

Таблиця 2

Структура віктимізації в мережі Інтернет

Вид діяння	% від загальної кількості респондентів
злом поштової скрині або акаунту у соцмережі	36 %
розповсюдження від мого імені неправдивої інформації	24 %
привласнення грошей інтернет-аферистами	4 %
пропозиція продажу неіснуючих товарів на платформах оголошень або у соцмережах	38 %
телефонні шахрайства або їх спроба	78 %
відвідування фішингових ресурсів, схожих на популярні Інтернет-магазини, банківські установи або організації	12 %
пропозиція переходу за сумнівними посиланнями	81 %
здійснення ризикованих онлайн-платежів	13 %
образи, спроби приниження	21 %
непристойні пропозиції, відправка інтимних фото	17 %
оформлення без моєї згоди платних інтернет підписок або спроба оформити	31 %

Результати дослідження свідчать, що близька 72% респондентів – осіб молодого віку, що кожен день відвідують мережу Інтернет, зіштовхувались із протиправними діями по відношенню до себе, або їх спробами в Інтернеті. Окрім цього опитування дає змогу прийти до висновку, що особи стикалися не з однією, а з декількома кіберзагрозами. Також ми приходимо до висновку про великий рівень латентності протиправних посягань, що вчиняються у кіберпросторі. Цифри офіційної статистики явно не відображають повний спектр таких дій. У зв'язку із цим, сьогодні особливо відчувається потреба у детальній розробці важливих питань, пов'язаних із віктимологічною характеристикою та запобіганням протиправним посяганням у кіберпросторі.

Також важливим тригером віктимізації молоді, особливо неповнолітніх в мережі Інтернет є прояви кібербулінгу, масштаби якого зростають кожен день, як зростає і рівень комунікації серед підлітків виключно у соціальних мережах та віртуальному просторі. Однак зазначене питання потребує окремого вивчення.

У підсумку слід підкреслити, що цілковите залучення населення до процесів цифровізації суспільства буде сприяти активізації їх віктимної поведінки, що, в свою чергу, вимагає від суб'єктів державної влади, громадських організацій, оперативних заходів віктимологічної профілактики кіберзлочинів, спрямованої, насамперед, на індивідуальне виховання неповнолітніх, підвищення рівня правосвідомості та технічної освіти в сфері кібербезпеки.

Список використаних джерел

1. Майже 23 млн. українців регулярно користуються Інтернетом. URL:<https://mind.ua/news/20204323-majzhe-23-mln-ukrayinciv-regulyarno-koristuyutsya-internetom-doslidzhennya> (дата звернення 19.10.2021).
2. Литвинов О.М., Орлов Ю.В. Нариси з кримінології постмодерну. Х. 2019. 278 с.
3. Report Serious Organised Crime (SOCTA/OCTA). URL:<https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment> (дата звернення 19.10.2021).
4. На Херсонщині поліцейські оголосили підозру організаторам шахрайського call-центру URL: <https://cyberpolice.gov.ua/news/na-xersonshhyni-policzejski-ogolosyly-pidozru-organizatoram-shaxrajnskogo-call-czentru-1108/> (дата звернення 19.10.2021).
5. Кіберполіція викрила киянина у привласненні грошей громадян через несанкціоноване втручання в роботу платіжних систем URL:<https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-kyuanyna-u-pryvlasnenni-groshej-gromadyan-cherez-nesankczionovane-vtruchannya-v-robotu-platizhnyx-system-4009/> (дата звернення 19.10.2021).
6. Джужа О.М. Віктимологія на захист прав і законних інтересів жертв злочину. Право України. 2002. №2. С. 134.
7. Джужа О. М. Запобігання злочинам: кримінологовіктимологічна парадигма. Київ. 2015. 331 с.
8. Всестороннее исследование проблемы киберпреступности : проект / С. Малби, Р. Мейс, А. Холтерхоф [и др.]. Вена, 2013. 360 с.
9. Литвинов О.М., Орлов Ю.В. Кримінологія «свого» часу: наукові розвідки. Харків. 2021. 316 с.

Одержано 01.05.2022