УДК 343.9:343.988
DOI https://doi.org/10.24144/2307-3322.2025.88.3.26

ВІКТИМОЛОГІЧНА ХАРАКТЕРИСТИКА ЖЕРТВ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ, ПЕРЕДБАЧЕНОГО СТ. 361 ККУ

Стручаєв М.Ф.,
аспірант кафедри кримінально-правової політики,
Національний юридичний університет імені Ярослава Мудрого
e-mail: admin@maxnet.ua

Стручаєв М.Ф. Віктимологічна характеристика жертв кримінального правопорушення, передбаченого ст. 361 ККУ.

У статті розглянуто питання віктимологічної характеристики осіб, які постраждали від кіберзлочинів, передбачених статтею 361 Кримінального кодексу України (несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж). Актуальність дослідження зумовлена стрімким зростанням кількості кіберзлочинів в умовах цифрової трансформації суспільства, а також низьким рівнем дослідження особистості потерпілого як об'єкта злочинного посягання. Метою статті є виявлення основних соціально-демографічних, психологічних та поведінкових характеристик осіб, які стають жертвами несанкціонованого втручання в роботу електронно-обчислювальних систем.

У процесі дослідження було застосовано комплексний методологічний підхід, який поєднує елементи системного, порівняльно-правового, статистичного та логіко-юридичного аналізу.

Проаналізовано чинне кримінальне законодавство України, статистичні дані правоохоронних органів, судову практику, а також практику розслідування кримінальних проваджень за статтею 361 КК України. Встановлено, що в більшості випадків потерпілими є особи віком від 21 до 45 років, з середнім або вищим рівнем освіти, є активними користувачами мережі Інтернет, зокрема соціальних мереж та онлайн-банкінгу. Характерною ознакою є необізнаність потерпілих щодо основ інформаційної безпеки, легковажне ставлення до збереження конфіденційної інформації та низький рівень цифрової гігієни.

Особливу увагу приділено аналізу психологічним характеристикам жертв кіберзлочинів, виявлено диференціацію потерпілих на активних та пасивних. Кожен тип характеризується певним набором психологічних ознак, так для активного типу притаманні екстравертованість, висока емоційна збудливість, сприйнятливість до зовнішніх впливів, прагнення до ризику, самовпевненістю. В свою чергу для пасивного - інтровертованість особистості, емоційна ригідність, підвищена тривожність, невпевненість у собі, схильність до замкнутості й уникнення конфліктів, що у поєднанні з низьким рівнем цифрової обізнаності створює передумови до їхньої віктимізації внаслідок недбалого користування інформаційними технологіями.

Отримані результати можуть стати основою для розробки нових профілактичних заходів, орієнтованих на зниження рівня віктимності серед населення.

Ключові слова: віктимологічна характеристика, особа потерпілого, кіберзлочинність, кримінологія, жертва злочину, психологічна характеристика.

Struchaiev M.F. Victimological characteristics of victims of a criminal offence under Article 361 of the Criminal Code of Ukraine.

The article explores the issue of the victimological profile of individuals who have suffered from cybercrimes stipulated under Article 361 of the Criminal Code of Ukraine (unauthorised interference with the operation of information (automated), electronic communications, information and communication systems, and electronic communications networks). The relevance of this study is driven by the rapid increase in cybercrime amid the digital transformation of society and the limited research on the

victim as an object of criminal encroachment. The purpose of this article is to identify the main socio-demographic, psychological, and behavioural characteristics of individuals who become victims of unauthorised interference with the functioning of electronic computing systems.

A comprehensive methodological approach has been applied in the course of the study, combining elements of systematic, comparative legal, statistical, and logical-legal analysis. The article examines current Ukrainian criminal legislation, statistical data from law enforcement agencies, judicial practice, and case studies of investigations conducted under Article 361 of the Criminal Code of Ukraine. It has been established that the majority of victims are individuals aged between 21 and 45, possessing either secondary or higher education, and actively using the Internet, particularly social networks and online banking platforms. A typical feature among these victims is a lack of awareness regarding information security fundamentals, a careless attitude towards the protection of confidential data, and poor digital hygiene practices.

Special attention is devoted to the psychological characteristics of cybercrime victims. The study identifies a differentiation between active and passive victims. Each type is characterised by a specific set of psychological traits. Active victims are typically extroverted, emotionally excitable, susceptible to external influences, prone to risk-taking, and often display overconfidence. Conversely, passive victims are usually introverted, emotionally rigid, highly anxious, lacking in self-confidence, inclined towards isolation, and tend to avoid conflict. When coupled with low levels of digital literacy, these traits contribute to their vulnerability and victimisation due to careless use of information technologies.

The findings of this study may serve as a foundation for the development of new preventive measures aimed at reducing the level of victimisation among the population.

Key words: victimological characteristics, victim's identity, cybercrime, criminology, crime victim, psychological profile.

Постановка проблеми. У сучасному світі інформаційні технології стали невід'ємною частиною усіх сфер життя – від побутових комунікацій до забезпечення функціонування складних державних і корпоративних систем. Разом із розвитком цифрового простору зростає і кількість кримінальних правопорушень, пов'язаних, зокрема, з несанкціонованим втручанням у роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [1, с. 145-146].

Так, у 2017 році відбулось стрімке погіршення криміногенної ситуації у сфері кібербезпеки, кількість злочинів передбачених ст. 361 КК збільшилась з 494 у 2016 р. до 1795 у 2017, у 2023 та 2024 роках їх кількість склала 2273 (2023) та 1953 (2024) кримінальних правопорушення [2, с. 117]. Крім того, варто одразу наголосити, що кіберзлочинність загалом має високий рівень латентності (95%), що свідчить про те, що кількість кримінальних правопорушень може буте значно більшою [3, с. 203–208].

Особливої уваги у цьому контексті потребує аналіз особи потерпілого – не лише як об'єкта посягання, а як активного елемента кримінологічної ситуації. Віктимологічне вивчення таких жертв дозволяє виявити характерні риси, моделі поведінки, рівень інформаційної захищеності, а також типові обставини, що сприяють вчиненню правопорушень. Саме формування віктимологічного портрета потерпілих може стати основою для розробки ефективних заходів попередження кіберзлочинів [4; 5].

Стан опрацювання проблематики. Теоретико-методологічні основи віктимології, поняття віктимності та сутність віктимологічної характеристики ґрунтовно досліджувалися у працях провідних вітчизняних науковців, зокрема Б.М. Головкіна, В.В. Голіна, А.Ф. Зелінського, О.В. Лисодєда та інших. У той же час, окремі аспекти віктимологічної характеристики кіберзлочинів були висвітлені у наукових роботах О.В. Фоменко, І.О. Коновалової, О.В. Голубєвої, Д.О. Шагірманова та А.А. Романюка. Водночас, слід наголосити, що питання віктимологічного аналізу кіберзлочинності потребує більш детального опрацювання кожного окремого виду кіберзлочинів, зокрема кримінального правопорушення передбаченого ст. 361 КК.

Метою даної статті є дослідження віктимологічних особливостей осіб, які стають жертвами несанкціонованого втручання в роботу електронно-обчислювальних машин, комп'ютерних систем і мереж, з урахуванням соціально-демографічних, поведінкових та професійних чинників [6, с. 3-4].

Виклад основного матеріалу. Віктимологічна характеристика представляє собою систему соціально-демографічних, психологічних, поведінкових та інших ознак особи потерпілого, що зумовлюють її віктимність, тобто здатність або схильність стати жертвою злочину.

Перш за все, важливо вказати, що даний злочин здебільшого не спрямований виключно проти фізичних осіб як таких, досить часто жертвами протиправних посягань стають юридичні особи та банківські установи, які активно використовують комп'ютерні системи, а також фізичні особи, важливою характеристикою яких є володіння або користування відповідними цифровими технологіями. Що стосується диференціації, то протягом 2019-2024 років дане кримінальне правопорушення було вчинене проти 113 фізичних осіб та 24 юридичних осіб, а загальна сума моральних та матеріальних збитків, завданих внаслідок вчинення злочину передбаченого ст. 361 КК склала 1 607 133 грн. (для фізичних осіб) та 362 849 (для юридичних) [7]. Це зумовлено, передусім, тим, що корпоративні структури зазвичай мають вищий рівень захисту інформаційних систем, зокрема застосування сучасних засобів кібербезпеки, багаторівневих протоколів автентифікації, систем резервного копіювання та спеціалізованих ІТ-відділів, які постійно моніторять стан інформаційної безпеки. Натомість фізичні особи в більшості випадків є менш захищеними у технічному та поведінковому аспектах, що підвищує їхню віктимність у цифровому середовищі та викликає необхідність їх віктимологічної характеристики.

Так, за статевою ознакою переважають чоловіки – 64,2%, водночас частка жінок за 2019-2024 р. становить 35,8%. Б.М. Головкін пояснює дану тенденцію злочинності із тим, що серед чоловічої частини населення порівняно більша частка осіб із віктимогенними деформаціями особистості, а також тих, хто з більшою вірогідністю може потрапити у злочинну ситуацію [6, с. 3]. У даному випадку також можна говорити про підвищений рівень зацікавленості чоловіків у цифрових технологіях, що зумовлює їхню постійну взаємодію з ними, та як наслідок, підвищує вірогідність стати жертвою несанкціонованого втручання або інших загроз. Так, станом на 2023 рік, чоловіки становили близько 74% фахівців у сфері інформаційних технологій [8]. Крім того, загальновідомо, що представники чоловічої статті частіше виявляють підвищений інтерес (іноді навіть азартний) до відеоігр, технічних пристроїв та інших інструментів, що забезпечують регулярну взаємодію із кіберпростором.

На жаль, у зв'язку з обмеженою доступністю статистичних даних, що надаються правоохоронними та судовими органами, встановлення вікової структури жертв є проблематичним. Згідно з даними Судової влади України, протягом останніх п'яти років зазначене кримінальне правопорушення було зафіксовано виключно стосовно повнолітніх осіб, що свідчить про відсутність осіб віком 13–17 років серед типових жертв. Водночас слід зауважити, що представники цієї вікової групи демонструють високий рівень інтеграції в цифровий простір, що потенційно підвищує ризик їх залучення до подібних інцидентів. Недостатній рівень довіри до дорослих, сприйняття ситуації як несуттєвої, або інші соціально-психологічні чинники можуть стати причиною неповідомлення про випадки несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних систем чи мереж, з боку неповнолітніх осіб.

Що стосується загальної диференціації, то за даними Національного бюро боротьби з шахрайством у Великобританії – жертвами кіберзлочинів схильні бути особи віком від 15 до 49 років [9, с. 329]. На нашу думку, виокремлення конкретної вікової групи серед потерпілих є недоцільним, оскільки при вчиненні кіберзлочину правопорушники скоріше орієнтуються на індивідуальні характеристики потенційної жертви, зокрема на рівень її рівень грамотності, поведінкові патерни у мережі, а також на ступінь дотримання елементарних принципів кібергігієни.

Разом із тим, вважаємо, що найбільшу частку серед жертв таких правопорушень становлять саме особи молодого та середнього віку (переважно 21–45 років). Це пояснюється високою активністю цієї категорії у цифровому середовищі, яка за відсутності належного рівня знань у сфері інформаційної безпеки або ігнорування ризиків, пов'язаних із недотриманням стандартів кібергігієни значно підвищує віктимність цієї вікової групи. Так, згідно з результатами дослідження, проведеного у 2023 році за підтримки Офісу Координатора допомоги США Європі та Євразії Державного департаменту США, найпоширенішою кіберзагрозою для цієї вікової групи є саме несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних та інформаційно-комунікаційних систем. Таке втручання часто реалізується шляхом отримання несанкціонованого доступу до облікових записів мобільних банківських додатків, онлайн-банкінгу, акаунтів у соціальних мережах тощо [10, с. 4].

Особи старшого віку хоч і не належать до типових жертв даного злочину, переважно через обмежену інтеграцію в цифровий простір - не можуть бути повністю виключені з групи ризику. Їх вразливість пояснюється, головним чином, низьким рівнем обізнаності у питаннях кібербезпеки, довірливістю та недостатнім усвідомленням потенційних загроз. Так, згідно з вищезгаданим дослідженням, лише 18% осіб віком до 60 років ознайомлені з основами кібербезпеки, тоді як серед респондентів віком понад 60 років цей показник становить лише 7%.

Задля визначення соціального статусу, рівня доходів та місця в суспільстві жертв несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж звернемось до Єдиного державного реєстру судових рішень. Так, у більшості вироків також фігурують статті 185, 190, 200 КК України, що свідчить про наявність у злочинця корисливого мотиву (74%) та переважно буденний характер вчинених злочинів. Б.М. Головкін стверджує, що жертвами загальнокримінальних правопорушень (зокрема крадіжок, грабежів, шахрайства) найчастіше стають особи із середнім рівнем доходів або навіть безробітні, які володіють виключно майном повсякденного вжитку. Така тенденція значною мірою зумовлена тим, що як злочинці, так і потерпілі, зазвичай належать до одного соціального прошарку, мають схожий стиль життя, подібні уявлення про рівень матеріального благополуччя. Їх об'єднує спільне соціальне становище, зокрема – маргіналізований статус, який характеризується соціальною вразливістю та периферійністю у загальній структурі суспільства.

За професійною ознакою та родом занять найбільший ризик віктимізації мають представники банківського та фінансового сектору (аналітики, бухгалтери, оператори банківських систем), працівники державних реєстрів та представники органів влади, адміністратори електронних журналів (мереж), журналісти, блогери, активісти, оператори мобільного зв'язку, інженери провайдерів та інші працівники телекомунікацій.

Також, визначення виключно соціально-демографічних характеристик потерпілого не є достатнім для повноцінного аналізу його ролі у злочинній ситуації та виявлення характеру взаємозв'язків із суб'єктом злочину. У зв'язку з цим особливої актуальності набуває вивчення психологічних особливостей особи жертви, які безпосередньо впливають на її поведінку в умовах криміногенної взаємодії та можуть зумовлювати її віктимну вразливість.

Умовно жертв даного злочину можна поділити на два типи — пасивний та активний. Пасивному типу властиві риси інтровертованої особистості: емоційна ригідність, підвищена тривожність, невпевненість у собі, схильність до замкнутості й уникнення конфліктів, що у поєднанні з низьким рівнем цифрової обізнаності створює передумови до їхньої віктимізації внаслідок недбалого користування інформаційними технологіями. Слід зазначити, що для цього типу потерпілих характерна переважно опосередкована або повністю відсутня взаємодія з правопорушником. Як правило, жертви стають об'єктами злочинного посягання внаслідок власних дій саме в цифровому світі (наприклад в мережі Інтернет) — зокрема, шляхом відкриття шкідливого електронного посилання чи файлу, за допомогою якого зловмисник отримує несанкціонований доступ до їхніх електронних пристроїв або інформаційних систем.

Активний тип жертв, навпаки, характеризується переважно екстравертованістю, високою емоційною збудливістю, сприйнятливістю до зовнішніх впливів, прагненням до ризику, самовпевненістю, а іноді – демонстративною зневагою до правил цифрової безпеки. Ці особи часто мають високий або середній рівень освіти, займають посади у сфері державної служби, бізнесу чи інформаційних технологій, демонструють підвищену довірливість у поєднанні з прагненням до швидкої вигоди, що може призводити до встановлення небезпечних контактів, використання ненадійного програмного забезпечення або недотримання базових принципів захисту інформації. Прикладом активної поведінки жертви може бути добровільне надання злочинцю свого телефону, паролів, тощо. Цікавим є той факт, що доволі часто жертви кримінального правопорушення передбаченого ст. 361 КК мають певні психологічні ознаки, які також притаманні для жертв шахрайства [11].

Висновок. Отже, в процесі дослідження було проведено віктимологічну характеристику жертв несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, визначено їх соціально-демографічні та психологічні ознаки, які дозволяють сформувати певний віктимологічний портрет та встановити взаємозв'язок між жертвою та злочинною ситуацією, або самим злочинцем.

Так, потерпілими від даного злочину можуть стати як фізичні, так і юридичні особи, однак саме фізичні особи залишаються менш захищеними як з технічної, так і з поведінкової точки зору. Типовими соціально-демографічними ознаками жертв таких правопорушень є: чоловіча стать, вік від 21 до 45 років, середній або високий рівень цифрової активності, професійна діяльність у сфері фінансів, державного управління, інформаційних технологій тощо.

Встановлено два основні типи жертв: пасивний – з ознаками інтровертованості, низької кіберграмотності, тривожності й уникання ризиків, та активний – з притаманними рисами екстравертованості, самовпевненості, прагненням до вигоди та неуважністю до правил кібербезпеки. Загалом ці психологічні характеристики разом із окресленими соціально-демографічними ознаками можуть бути використані для ідентифікації вразливих груп населення та розробки цільових програм превенції даного кримінального правопорушення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Таволжанський О.В. Деякі актуальні аспекти сучасної кримінально-правової політики в сфері забезпечення кібербезпеки України. *Актуальні проблеми протидії злочинності та корупції: збірник тез Всеукраїнської науково-практичної конференції.* Харків: Юрайт. 2023. С. 145–150.
2. Таволжанський О.В. Сучасні реалії кіберпростору України. *Забезпечення правопорядку в умовах коронакризи: матеріали панельної дискусії IV Харків. міжнар. юрид. форуму, м. Харків, 23–24 верес. 2020 р*. Харків, 2020. С. 203–208.
3. Стручаєв М.В. Кримінологічний аналіз злочинності за ст. 361 КК України: статистичні закономірності та тенденції. The 3rd International Scientific and Practical Conference «Scientific Exploration: Bridging Theory and Practice» (March 24-26, 2025. Berlin, Germany). European Open Science Space. 2025. С. 116–120.
4. Віктимологія: навч. посібник / за ред. Голіни В.В., Головкіна Б.М. Харків: Право, 2017. 343 с.
5. Holovkin B., Cherniavskyi S., Tavolzhanskyi O. Factors of Cybercrime in Ukraine. *Relações Internacionais no Mundo Atual*. 2022. Vol. 3, № 41. 25 с.
6. Головкін Б.М. Віктимізація населення в Україні: стан, детермінанти, запобігання. *Теорія і практика законодавства*. 2014. Вип. 2 (6). С. 1–13є
7. Звіт судів першої інстанції про розгляд матеріалів кримінального провадження (2019–2024). Судова влада України. URL: https://court.gov.ua/inshe/ sudova_statystyka/zvit_dsau_2024.
8. Портрет IT-спеціаліста — 2023. Аналітика. Інтернет-ресурс: https://dou.ua/lenta/articles/ portrait-2023.
9. Фоменко О.В. Кіберзлочинність: сучасний стан та особливості віктимологічної профілактики. *Юридичний науковий електронний журнал*. 2017. № 6. С. 328–330.
10. Звіт про проміжне дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки. Підготовлено для CRDF Global. Дослідження проведено за підтримки Офісу Державного департаменту США Координатора допомоги США Європі та Євразії. 2023. 75 с.
11. Головкін Б.М. Віктимність як основна категорія віктимології. *Журнал східноєвропейського права*. 2015. № 20. С. 6–13.