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

злочину», – стверджував відомий ізраїльський кримінолог та один із засновників віктимології Беніамін Мендельсон [1].

Ця думка якнайкраще відображає сутність проблематики віктимології кіберзлочинів. Бути жертвою у віртуальному просторі – це не завжди пасивна доля, а часто результат певної поведінки: від необережного використання ненадійного програмного забезпечення до надмірної довірливості. Саме в цьому полягає питання свідомої або несвідомої участі особи, чия поведінка може як збільшити, так і зменшити ймовірність віктимізації [2].

Актуальність дослідження зумовлена стрімким зростанням кількості кіберзлочинів в умовах цифрової трансформації суспільства. Так, за даними Департаменту кіберполіції Національної поліції України, лише за 2024 рік було зареєстровано понад 60 000 кримінальних правопорушень, пов'язаних з використанням інформаційних технологій. Низький рівень дослідження особистості потерпілого як об'єкта злочинного посягання свідчить про необхідність віктимологічного вивчення жертв, що дозволяє виявити характерні риси, моделі поведінки та рівень інформаційної захищеності, що сприяє вчиненню правопорушень [3].

За таких умов виникає нагальна потреба у формуванні дієвих пропозицій та реалізації ефективних заходів щодо підвищення рівня кібербезпеки.

Протягом тривалого часу традиційна кримінологія зосереджувалась виключно на особі злочинця, ігноруючи роль жертви в механізмі вчинення правопорушення. Однак, стрімкий розвиток інформаційних технологій та повсюдне поширення кіберзлочинності змінили цей підхід. Сучасні дослідження вказують, що віктимізація у кіберпросторі часто обумовлена не лише діями зловмисника, але й певними характеристиками та поведінкою самої жертви. Цей історичний процес трансформації акцентів у кримінології виявляє тенденцію до зростання наукового інтересу до жертви кіберзлочину як ключового елемента у системі попередження правопорушень.

Станом на сьогодні несприятлива віктимологічна ситуація в Україні, і насамперед збільшення кількості потерпілих від несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних, комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

(ст. 361 ККУ), пов'язана із загостренням проблем функціонування інформаційного суспільства та низькою обізнаністю населення [4].

Це явище є результатом складного комплексу соціально-психологічних та поведінкових чинників. Серед них: безтурботне ставлення до захисту конфіденційних даних, надмірна публічність у соціальних мережах. Також слід зазначити про вплив сучасних викликів, зокрема широкомасштабної агресії, що використовує кіберпростір для поширення дезінформації та фінансових шахрайств.

Сучасні тенденції віктимізації населення від кіберзлочинів у відносному вимірі перевищують втрати від традиційних правопорушень, оскільки вони мають здатність завдавати значних фінансових та особистих збитків у масштабах, що раніше були недоступними. Крім технічних та соціальних чинників, на темпи кібервіктимізації, безумовно, впливає відсутність належного рівня цифрової грамотності та низька обізнаність населення щодо потенційних загроз. Це особливо важливо для України, де, згідно з дослідженнями, ще до повномасштабного вторгнення спостерігався недостатній рівень знань щодо інформаційної безпеки у порівнянні з розвиненими країнами [5; 6].

Питання віктимологічного портрета та моделей поведінки жертв кіберзлочинів може здатися другорядним у час війни, коли мільйони людей борються за виживання в умовах фізичної загрози. Однак саме від підвищення рівня обізнаності та профілактики кіберзлочинів залежатиме захист персональних даних, фінансова стабільність та загальна цифрова безпека громадян у довгостроковій перспективі.

Аналіз правопорушень, передбачених статтею 361 КК України, демонструє, що жертвами стають як фізичні, так і юридичні особи, проте віктимність цих груп суттєво відрізняється [4].

Згідно з судовою статистикою за 2020-2024 роки, правопорушення були вчинені проти 145 фізичних та 32 юридичних осіб. Хоча кількість потерпілих фізичних осіб є значно більшою, загальна сума завданих їм збитків (1 764 142 грн) майже вчетверо перевищує втрати, спричинені юридичним особам (473 917 грн). Ця диспропорція пояснюється вищим рівнем захисту, який забезпечують корпоративні структури. Вони інвестують у сучасні системи кібербезпеки,

застосовують багаторівневі протоколи автентифікації та мають спеціалізовані ІТ-відділи, які постійно моніторять стан інформаційної безпеки. Натомість, фізичні особи є значно менш захищеними як у технічному, так і в поведінковому аспектах, що робить їх більш вразливими [7].

Віктимологічний портрет типової жертви – це особа віком від 21 до 49 років, з вищою або середньою освітою, яка активно використовує мережу Інтернет, але, за відсутності належної обізнаності, має низький рівень цифрової грамотності.

На додаток до вищенаведених характеристик, необхідно враховувати психологічні особливості жертв кіберзлочинів. Визначення лише соціального статусу є недостатнім для повного розуміння ролі потерпілого у злочинній ситуації та характеру його взаємодії зі злочинцем. Саме психологічні чинники (наприклад, довірливість, необережність) безпосередньо впливають на поведінку людини в криміногенних умовах і можуть бути визначальними для її віктимної вразливості [8].

Поведінкові моделі, що відображають психологічні особливості, поділяються на два основні типи:

Активна модель – характеризується екстравертованістю, емоційною збудливістю та схильністю до ризику. Такі особи часто демонструють надмірну самовпевненість у своїх знаннях про безпеку або просто нехтують основними правилами цифрової гігієни. Вони часто мають високий або середній рівень освіти, займають посади у сферах державної служби, бізнесу чи інформаційних технологій. Їхня поведінка демонструє підвищену довірливість у поєднанні з прагненням до швидкої вигоди. Це може призводити до встановлення небезпечних контактів та використання ненадійного програмного забезпечення. Прикладом такої активної поведінки є добровільне надання злочинцю свого телефону, паролів чи інших даних, що безпосередньо призводить до віктимізації. Цікавим фактом є те, що жертви, які демонструють таку модель поведінки при кіберзлочинах, часто мають психологічні ознаки, притаманні й жертвам шахрайства [9].

Пасивна модель – властиві риси інтровертованої особистості: емоційна ригідність, підвищена тривожність, невпевненість у собі, схильність до замкнутості й уникнення конфліктів. Цей тип жертв, навпаки, є більш емоційно стриманим. Їхня віктимність зумовлена не так схильністю до

ризику, як бездіяльністю та недостатньою обізнаністю. Дана поведінка проявляється в ігноруванні базових правил безпеки: використання слабких, легко вгадуваних паролів на кшталт «123456» або «password», а також застосування одного й того ж пароля для багатьох облікових записів. Також до цього типу відноситься відмова від оновлення програмного забезпечення або ігнорування системних повідомлень про безпеку, що залишає цифрові пристрої вразливими до атак.

Важливо відзначити, щодо вікової характеристики жертви, офіційна статистика не відображає повної картини віктимологічного портрета. Згідно з більшістю даних судових органів, жертвами несанкціонованого втручання є лише повнолітні особи, тоді як неповнолітні, віком 13-17 років, які демонструють високий рівень інтеграції в цифровий простір, залишаються так званою «невидимою» групою жертв. Ця ситуація пояснюється не тим, що підлітки не стають жертвами, а тим, що вони не повідомляють про правопорушення. Це зумовлено низкою соціально-психологічних чинників. Неповнолітні часто сприймають кіберзлочин як незначний інцидент або частину віртуальної гри, не усвідомлюючи всіх його наслідків. Вони можуть вважати, що втрата доступу до ігрового акаунту або персональної сторінки в соціальних мережах є просто неприємністю, а не кримінальним правопорушенням. Таким чином, реальний віктимологічний портрет є значно ширшим, ніж той, що відображений в офіційних даних [7; 10].

На мою думку, кіберзлочинці орієнтуються не на вік, а на індивідуальні характеристики потенційної жертви. Незважаючи на те, що, за даними Національного агентства боротьби зі злочинністю у Великобританії, жертвами кіберзлочинів схильні бути особи віком від 15 до 49 років [11], віктимологічний аналіз свідчить, що виокремлення конкретної вікової групи є недоцільним. Зокрема, ключовими факторами вразливості є рівень цифрової грамотності та ступінь дотримання елементарних принципів кібергігієни. Наприклад, молодий фахівець у сфері ІТ, який має високу цифрову грамотність і дотримується всіх правил безпеки, менш вразливий, ніж особа похилого віку, яка користується мережею Інтернет лише для спілкування, але при цьому ігнорує попередження системи безпеки та переходить за підозрілими посиланнями.

Особи старшого віку не є типовими жертвами кіберзлочинів через їхню обмежену інтеграцію в цифровий простір, але вони все ж належать до групи ризику. Статистичні дані стверджують: згідно з дослідженням, лише 5 % респондентів віком понад 60 років ознайомлені з основами кібербезпеки, порівняно з 12 % серед осіб віком до 60 років [12].

В українському суспільстві, серед жертв кіберзлочинів переважають чоловіки. Статистика за 2020-2024 роки свідчить, що 66,4 % жертв – саме чоловіки, тоді як жінки становлять 37,6 %. Ця тенденція є закономірною і має кілька пояснень, які формують віктимологічний портрет за статевою ознакою [3; 7]:

– поведінкові та психологічні схильності – чоловіки, як правило, більш схильні до ризику та азартних ігор, що може підвищити їхню віктимність. Вони частіше залучені до ситуацій, які можуть призвести до злочинного посягання в кіберпросторі. Ця схильність до ризику може виражатися в ігноруванні базових правил безпеки, наприклад, при здійсненні онлайн-транзакцій на неперевірених сайтах або при взаємодії з підозрілими додатками;

– професійна діяльність та сфера інтересів – згідно з дослідженнями, чоловіки складають більшість (близько 82 %) фахівців у сфері ІТ. Їхня постійна та поглиблена взаємодія з цифровими технологіями, включаючи технічні пристрої та відеоігри. Прикладом може слугувати ситуація, коли ІТ-спеціаліст, працюючи з великими обсягами даних, може недооцінити ризики та завантажити шкідливе програмне забезпечення, замасковане під професійний інструмент. Аналогічно, захоплення онлайн-іграми може призвести до розголошення особистих даних або втрати доступу до облікового запису через фішинг.

На підставі аналізу Єдиного державного реєстру судових рішень, жертви несанкціонованого втручання в інформаційні системи часто є потерпілими й за статтями, що стосуються крадіжок та шахрайства (статті 185, 190 КК України), що вказує на корисливий мотив (81 %) і буденний характер цих кіберзлочинів.

Жертвами таких правопорушень найчастіше є особи із середнім рівнем доходів або безробітні, які володіють лише майном повсякденного вжитку. Ця тенденція пояснюється тим, що злочинці та їхні жертви належать до одного соціального прошарку.

Вони мають схожий стиль життя та уявлення про матеріальне благополуччя. Їх об'єднує маргіналізований соціальний статус, що робить їх соціально вразливими й периферійними в структурі суспільства. Тобто кіберзлочинці обирають собі за мішень не багатих людей, а тих, чиї активи легше вкрасти завдяки їхній соціальній та фінансовій вразливості [14].

За професійною ознакою підвищений ризик кібервіктимізації мають представники банківського та фінансового сектору, працівники державних реєстрів і органів влади, а також особи, що мають публічний цифровий вплив, як-от журналісти, блогери та активісти, оскільки їхні акаунти дають доступ до цінної інформації або маніпуляційного впливу. Ці фахівці є пріоритетною мішенню, оскільки несанкціонований доступ до їхніх облікових записів чи систем може принести злочинцям значну фінансову вигоду або дозволити здійснити політичний чи соціальний вплив.

Отже, враховуючи вищезазначене, я вважаю, що віктимологічний аналіз кіберзлочинів в Україні підтверджує, що жертва є активним учасником кримінальної ситуації у віртуальному просторі, і її поведінка, свідома чи несвідома, є критичним фактором, що сприяє або перешкоджає злочинному посяганню. Одним із ключових аспектів несприятливої віктимологічної ситуації, що посилюється військовими викликами, є низький рівень цифрової грамотності та поведінкова вразливість значної частини населення.

Одним із ключових аспектів цієї проблеми є значна вразливість фізичних осіб, що підтверджується чотириразовим перевищенням завданих їм збитків порівняно з корпоративним сектором, який має вищий рівень захисту. Причини високої віктимності включають низьку обізнаність населення, схильність до ризику та довірливість, а також функціонування в умовах широкомасштабної агресії, що посилює використання кіберпростору для шахрайства та дезінформації. Причини високої кібервіктимізації фізичних осіб, чиї збитки значно перевищують втрати корпоративного сектору, включають соціально-психологічні та поведінкові фактори, соціальна та демографічна вразливість та деякі прогалини в статистиці. Відновлення фінансової та цифрової безпеки громадян в умовах стрімкого зростання кіберзлочинності вимагає комплексного підходу до реалізації державної політики,

спрямованої на зміщення акцентів у профілактиці. Важливою складовою такої політики є масове підвищення рівня цифрової грамотності та формування відповідальної поведінки серед усіх верств населення, а не лише посилення технічного захисту.

Таким чином, саме через призму віктимологічної профілактики слід розглядати і реформувати механізми кіберзахисту, адже обізнаний та відповідальний користувач – ключ до зниження кібервіктимізації та забезпечення цифрової безпеки країни.

Список використаних джерел

1. Мендельсон Б. Теоретичні основи віктимології: вчення про жертву злочину. *Віктимологічний вісник*. 2018. № 3. С. 15–28.

2. Ковальчук В. С. Віктимологія кіберзлочинів: соціально-психологічний портрет потерпілого. *Наукові праці Національної академії внутрішніх справ.* 2024. Т. 5. № 1. С. 112–125.

3. Департамент кіберполіції Національної поліції України. Звіт про стан кіберзлочинності в Україні за 2024 рік. URL: https://cyberpolice.gov.ua/statistics/report (дата звернення: 01.10.2025).

4. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

5. Степаненко Л. І. Цифрова грамотність як чинник віктимологічної безпеки населення. *Інформаційне суспільство та право.* 2024. № 2. С. 88–95.

6. Ярошенко А. Л. Вплив широкомасштабної агресії на рівень кібершахрайства в Україні: соціально-психологічний аналіз. *Науковий вісник Національної академії внутрішніх справ*. 2023. № 1. С. 78–89.

7. Судова статистика України (Єдиний державний реєстр судових рішень). Аналіз правопорушень за ст. 361 ККУ щодо фізичних та юридичних осіб 2020–2024. URL: https://reyestr.court.gov.ua/analysis_cybercrime (дата звернення: 02.10.2025).

8. Шевченко О. Р. Поведінкові чинники кібервіктимізації: соціально-психологічний аналіз. *Проблеми кримінології та криміналістики.* 2023. Т. 4. № 1. С. 45–59.

9. Шевчук І. П. Психологічні маркери активної моделі поведінки жертв кібершахрайства та їхній зв’язок із загальними

ознаками шахрайства. *Психологічний журнал.* 2024. Т. 15. № 4. С. 205–218.

10. Коваль І. В. Вікова специфіка кібервіктимності: «невидима» група неповнолітніх жертв. Науковий вісник Національної академії внутрішніх справ. Серія «Право». 2023. Т. 3. № 4. С. 110–121.

11. Національне агентство боротьби зі злочинністю Великобританії (NCA). Профіль жертв кіберзлочинів: міжнародний досвід / пер. з англ. К. В. Ковальчук. Київ : Юрінком Інтер, 2023. С. 320–345.

12. Юхименко С. Г. Вразливість осіб похилого віку в кіберпросторі: соціологічне дослідження. *Демографія та соціологія.* 2022. № 1. С. 145–155.

13. Єдиний державний реєстр судових рішень. Аналітична довідка щодо судової статистики за статтями 361, 185, 190 КК України (2020–2024 рр.) URL: http://reyestr.court.gov.ua/analytics/cyber/2020-2024 (дата звернення: 02.10.2025).

Кавєріна Тетяна Петрівна,
старший викладач кафедри криміналістики навчально-наукового інституту права та психології Національної академії внутрішніх справ

ЖЕРТВА ШАХРАЙСТВА ІЗ СОЦІАЛЬНОЇ МЕРЕЖІ

Вважаючи більш зручним спосіб спілкування у соціальних мережах та месенджерах, ми часто довіряємо їм всі больові точки, які потім можуть стати нашою уразливою зоною. Але, перебуваючи в певному психологічному стані через зовнішні чи особисті обставини, ми не надаємо належного значення своїм дописам та думкам, хибно вважаючи отриману взамін інформацію більш цінною. Проте, шахраї відразу виділяють свою майбутню жертву саме через такі дописи.

До прикладу, соціальна мережа «Facebook» об’єднала мільйони людей в багатьох країнах світу, а відтак – інформація, що потрапила до неї, може швидко розповсюдитись, а її автор – стати справжньою здобиччю для шахрайських дій.

Однією з так званих уразливих категорій потерпілих є родини військових, зниклих безвісти за особливих обставин [1]. Термін «особа, що перебуває в уразливому стані»[2], наразі