

ПОНЯТТЯ ТА КВАЛІФІКАЦІЙНІ ОЗНАКИ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ «КІБЕРЕКСПЛУАТАЦІЯ ЛЮДИНИ»

CONCEPTS AND QUALIFICATIONS OF THE CRIMINAL ACT OF "CYBER EXPLOITATION OF HUMAN BEINGS"

Христюк В.В., аспірантка кафедри національного, міжнародного права
та правоохоронної діяльності
Херсонський державний університет

У статті запропоновано та розглядається поняття та кваліфікаційні ознаки такого кримінального правопорушення як «кіберексплуатація людини», що виступає як специфічна форма кримінального правопорушення у сфері незаконної експлуатації людини. Метою дослідження є виявлення та систематизація особливостей цього кримінального правопорушення у сфері експлуатації людини в умовах інформаційного суспільства, а також розробка рекомендацій щодо його правової кваліфікації та правозастосування. Для досягнення поставлених цілей використано методи правового аналізу та компаративістики. Дослідження базується на аналізі національного законодавства, судової практики, а також міжнародних стандартів у сфері прав людини та боротьби з кіберзлочинністю. У результаті дослідження запропоновано поняття «кіберексплуатація людини», проаналізовано та здійснено порівняння таких понять як «кібербулінг», «онлайн-експлуатація» [1], «кібершахрайство».

Для досягнення мети наукового дослідження шляхом правового аналізу у статті висвітлено кваліфікаційні ознаки кримінального правопорушення «кіберексплуатація людини», запропоновано межі обвинувачення та межі доказування, визначено можливі ролі осіб, які є учасниками кримінального правопорушення.

У результаті дослідження «кіберексплуатацію люди» визначено як протиправне використання особи з метою отримання незаконної вигоди або заподіяння шкоди, вчинене за допомогою інформаційно-комунікаційних технологій. Основними кваліфікаційними ознаками цього злочину є: використання інформаційних технологій для залучення, контролю або експлуатації особи; наявність прямого умислу щодо отримання вигоди; порушення прав та свобод людини.

Кіберексплуатація людини є складним явищем, тісно пов'язаним з іншими злочинами у сфері незаконної експлуатації, і потребує чіткого правового визначення та відповідного законодавчого регулювання. Дослідження підкреслює важливість вдосконалення національних норм та міжнародних стандартів, які регулюють цю сферу, з метою забезпечення ефективної боротьби з кіберзлочинністю та захисту прав людини в умовах глобалізації. Результати дослідження можуть слугувати основою для подальших наукових розробок у царині кримінального права та інформаційної безпеки.

Ключові слова: кіберексплуатація, інформаційна безпека, незаконна експлуатація людини, правова кваліфікація, межі обвинувачення.

The article proposes and examines the concept and qualifying features of such a criminal offense as "cyberexploitation of a person", which acts as a specific form of a criminal offense in the field of illegal exploitation of a person. The purpose of the study is to identify and systematize the features of this criminal offense in the conditions of the information society, as well as to develop recommendations regarding its legal qualification and enforcement. The methods of legal analysis and comparative studies were used to achieve the set goals. The research is based on the analysis of national legislation, judicial practice, as well as international standards in the field of human rights and combating cybercrime. As a result of the study, the concept of "cyberexploitation of a person" was proposed, such concepts as "cyberbullying", "online exploitation", "cyberfraud" were analyzed and compared.

To achieve the goal of scientific research through legal analysis, the article highlights the qualifying features of the criminal offense "cyberexploitation of a person", proposes the limits of accusation and the limits of proof, defines the possible roles of persons who are participants in the criminal offense.

As a result of the study, "cyberexploitation of people" is defined as the illegal use of a person for the purpose of obtaining an illegal benefit or causing harm, committed with the help of information and communication technologies. The main qualifying features of this crime are: use of information technology to attract, control or exploit a person; the presence of a direct intention to obtain a benefit; violation of human rights and freedoms.

Cyber exploitation of a person is a complex phenomenon, closely related to other crimes in the field of illegal exploitation, and requires a clear legal definition and appropriate legislative regulation. The study emphasizes the importance of improving national norms and international standards that regulate this area, in order to ensure the effective fight against cybercrime and the protection of human rights in the context of globalization. The results of the study can serve as a basis for further scientific developments in the field of criminal law and information security.

Key words: cyber exploitation, information security, illegal human exploitation, legal qualification, limits of prosecution.

Постановка та актуальність проблеми. У сучасному цифровому середовищі, яке характеризується інтенсивним розвитком інформаційних технологій, відзначається зростання загроз кіберексплуатації людини, тобто дії зловмисного характеру у віртуальному просторі, які можуть призвести до серйозних порушень прав та гідності людини.

Аналізом останніх досліджень і публікацій нами встановлено, що поняття «кіберзлочинності» у сфері інформаційної безпеки стало об'єктом дослідження у працях багатьох українських та зарубіжних науковців, зокрема, таких як Д. С. Азаров, П. Д. Біленчук, В. А. Глушков, Н. А. Гуторова, Н. В. Карчевський, Н. І. Хавронюк, В. І. Алескеров, В. Б. Вехов, М. А. Сфремова, тощо, проте, у науковому просторі не відображені будь-які дослідження дотичних питань цієї статті, що також входить у постановку проблеми статті.

Метою статті є виявлення та систематизація особливостей кримінального правопорушення у сфері експлуата-

ції людини в умовах інформаційного суспільства, а також розробка рекомендацій щодо його правової кваліфікації та правозастосування.

Для досягнення поставлених цілей використано **методи** правового аналізу та компаративістики.

Виклад матеріалу дослідження та його основні результати. Поняття «кіберексплуатація людини», «експлуатація у віртуальних середовищах» та «експлуатація через соціальні мережі» набувають актуальності і вимагають детального аналізу та правової кваліфікації.

Аналіз цих явищ є особливо важливим у зв'язку зі зростанням кіберзлочинності та необхідністю розробки ефективних механізмів правового захисту в цифровій сфері та незаконної експлуатації людини.

Дослідження спрямоване на виявлення основних ознак кримінального правопорушення «кіберексплуатації людини» та розкриття їхнього правового статусу в кон-

тексті кримінального права, що є необхідним для забезпечення належного захисту прав та інтересів осіб, які стають жертвами зазначених злочинів.

З огляду на поширення сучасних технологій та їх вплив на соціальні відносини, нові форми експлуатації людини можуть включати кіберексплуатацію, експлуатацію людини у віртуальних середовищах, експлуатацію через соціальні мережі.

Кіберексплуатація може передбачати дії особи або юридичної особи, які використовують технології та мережі Інтернет з метою незаконної експлуатації інших осіб. Це можуть бути такі дії як шахрайство, маніпуляції та контроль за особою інформацією. У рамках правового розуміння термін «кіберексплуатація» охоплює зловживання особою або юридичною особою технологіями та Інтернетом для здійснення контролю, шахрайства, маніпуляцій або залучення осіб у цифровому середовищі з метою отримання неправомірної вигоди чи завдання шкоди.

Експлуатація у віртуальних середовищах. Використання віртуальної реальності та онлайн-ігор може призводити до ситуацій, коли особа стає жертвою експлуатації у цифровому середовищі. Це може включати залучення до віртуальних мереж проституції або торгівлі людьми. У рамках правового розуміння термін «експлуатація у віртуальних середовищах» може описувати зловживання та незаконне використання інформаційно-комунікаційних технологій, онлайн-платформ для залучення, контролю або експлуатації осіб. Це охоплює широкий спектр дій, зокрема, експлуатацію дітей у віртуальних середовищах, онлайн-шахрайство, кібербулінг, сексуальну експлуатацію через інтернет, фінансові шахрайства та інші злочини, що вчиняються за допомогою цифрових технологій.

Під формою «експлуатація через соціальні мережі» можемо розуміти зловживання соціальними мережами для залучення та контролю над особами, зокрема неповнолітніми, яке може призводити до їх експлуатації у різних формах, включаючи сексуальне використання, торгівлю людьми та залучення до кримінальних груп. Така форма може включати в себе широкий спектр дій, таких як залучення осіб до незаконних діяльностей через соціальні мережі, рекрутація осіб для злочинних організацій або груп, використання соціальних мереж для здійснення фінансових або сексуальних злочинів, шахрайство через соціальні мережі та інші злочинні дії, які здійснюються за допомогою цифрових платформ для спілкування та взаємодії.

Аналізуючи широке поле правозастосування варіантів вживання термінів, нами визначено єдине поняття «кіберексплуатація людини», яке охоплює вищевикладені підкатегорії.

Отже, кіберексплуатація людини може визначається як використання інформаційних технологій та мережі Інтернет для незаконної експлуатації особи з метою отримання неправомірної вигоди або завдання шкоди. Таке поняття є широким, яке включає різноманітні дії та злочинні сценарії, що реалізуються у віртуальному просторі.

Для досягнення мети та повноти наукового дослідження, вважаємо, що необхідно чітко визначити межі обвинувачення у справах, пов'язаних з кіберексплуатацією людини.

По-перше, таке кримінальне правопорушення охоплює дії, що включають, але не обмежуються, формами: зловживання інформаційними технологіями для здійснення контролю над особою; використання ресурсів Інтернету для шахрайства, маніпуляцій або обману; участь у торгівлі людьми або сексуальній експлуатації через онлайн-платформи; використання соціальних мереж для розповсюдження дезінформації з метою шкоди особі [4, с. 846].

Таким чином, поняття «кіберексплуатація людини» є важливим предметом дослідження в контексті сучасного кримінального права, що вимагає детального аналізу

та розробки правових механізмів для ефективного протидії цим правопорушенням.

Окрім того, визначення меж обвинувачення є критично важливим етапом наукового дослідження, особливо в контексті вивчення кримінальних правопорушень. По-перше, чітке окреслення меж обвинувачення дозволяє забезпечити правову визначеність та стабільність у системі кримінального правосуддя. Це є необхідним для формування єдиного підходу до кваліфікації злочинів, що у свою чергу сприяє запобіганню правових колізій і підвищенню ефективності правозастосування.

По-друге, визначення меж обвинувачення дозволяє детально дослідити специфіку та різноманітність дій, що підпадають під поняття кіберексплуатації. Це включає в себе не лише встановлення характеру злочинних дій, а й аналіз причинно-наслідкових зв'язків між діями злочинця і стражданнями жертв. Таке глибоке розуміння дозволяє формувати обвинувачення на основі об'єктивних критеріїв, що враховують специфіку цифрового середовища.

По-третє, межі обвинувачення є основою для розробки ефективних механізмів правового захисту та реагування з боку правоохоронних органів. Це включає формування оперативних стратегій, направлених на профілактику та викриття кіберзлочинів, а також забезпечення прав потерпілих.

Врешті-решт, чітке визначення меж обвинувачення в наукових дослідженнях сприяє розвитку кримінальної політики та законодавства, а також підвищує обізнаність суспільства про природу і масштаби кіберексплуатації, що в свою чергу впливає на формування більш обґрунтованих підходів до її регулювання. Таким чином, даний аспект є ключовим для забезпечення комплексного та ефективного реагування на виклики, які ставить сучасний цифровий простір, зокрема у сфері експлуатації людини.

Межі обвинувачення у справах, пов'язаних із кіберексплуатацією людини, визначаються конкретними діями, які включають, але не обмежуються: онлайн-шахрайство та обман; залучення осіб до шахрайських схем через Інтернет, зокрема фішингові атаки, вірусні спам-повідомлення, підроблені веб-сайти та інші маніпулятивні дії, що мають на меті отримання організатором конфіденційної інформації або фінансових ресурсів.

Кібербулінг та онлайн-експлуатація можуть виражатися у систематичному насильстві, залякуванні або психологічному тиску на особу через соціальні мережі, форуми, чати тощо, що призводить до психологічних травм та/або соціальної ізоляції жертви [5].

Згідно з дослідженням, проведеним Інститутом масової інформації, кібербулінг є однією з найпоширеніших форм онлайн-насильства, що включає систематичне переслідування, приниження та залякування осіб через цифрові платформи та соціальні мережі [1].

Експлуатація через соціальні мережі можуть виражатися через залучення осіб до незаконних дій або груп через платформи соціальних мереж з метою експлуатації, контролю або фінансової маніпуляції, що підриває основи особистої автономії і безпеки жертви [4, с. 847].

Віртуальна експлуатація ж у використанні віртуальної реальності та онлайн-ігор для залучення осіб до незаконних дій або експлуатації у цифровому середовищі, що може включати, зокрема, примусові дії та маніпуляції.

Кримінальні дії, пов'язані з кіберексплуатацією людини, є складними та багатогранними. Вони можуть включати різні види злочинних дій, що реалізуються у цифровому середовищі, і вимагають глибокого розуміння ролей кожної особи, залученої до цих злочинів.

У сучасному цифровому середовищі кіберексплуатація демонструє зростаючу тенденцію поширення, зокрема, через організовані злочинні схеми, які використовують онлайн-платформи для шахрайства. Одним з характерних

прикладів кіберексплуатації є ситуація, коли організатори залучають інших осіб для розміщення фіктивних оголошень про продаж товарів чи послуг на інтернет-ресурсах, таких як сайт ОЛХ.

Для праворозуміння та визначення специфіки кримінального правопорушення, на нашу думку, необхідно розібрати наступний приклад: «ОСОБА-1, що виступає як організатор, відповідає за планування та координацію шахрайської схеми, наймає ОСОБА-2, яка виконуватиме роль виконавця, публікуючи фіктивні оголошення на платформі ОЛХ. ОСОБА-1 надає інформацію та фотографії товарів для публікації, а ОСОБА-2 реалізує цю задачу, вказуючи контактні дані організатора. Оголошення мають на меті залучення потенційних покупців, які, покладаючись на добросовісність угоди, перераховують кошти на придбання товару. Проте, товар не надсилається, і покупець стає жертвою шахрайської діяльності. Важливо зазначити, що ОСОБА-1 усвідомлює відсутність товару, проте продовжує керувати шахрайською схемою для отримання особистої вигоди».

В цій ситуації ОСОБА-1 несе відповідальність за організацію та управління шахрайською схемою, що відносить її до категорії організаторів кіберексплуатації. Відповідно, вона може бути обвинувачена у скоєнні злочину, пов'язаного з кіберексплуатацією. Водночас, ОСОБА-2, яка здійснює публікацію оголошень, може бути розглянута як потерпіла особа в даному контексті, оскільки її дії виконуються на підставі вказівок організатора, і вона не має повного усвідомлення наслідків своїх дій.

Межі обвинувачення щодо організатора в цій ситуації базуються на доведенні наміру вчинити кіберексплуатацію, активної участі в плануванні та координації злочинної схеми, а також усвідомленні наслідків своїх дій. Відповідно, обвинувачення повинно продемонструвати, що ОСОБА-1 свідомо планувала і організовувала схему з метою отримання вигоди. Це може бути підтверджено через наявність попередніх планів, комунікацій з співучасниками або відповідних записів, що свідчать про намір ОСОБА-1.

Крім того, обвинувачення має продемонструвати активну участь ОСОБА-1 у плануванні та координації злочинної схеми, що може включати організацію зустрічей, розподіл ролей, надання інструкцій і нагляд за виконанням завдань. Ця інформація може бути підтверджена електронними комунікаціями, записами телефонних розмов, фінансовими транзакціями та іншими доказами, які свідчать про активну участь ОСОБА-1 у реалізації схеми.

Окрім того, необхідно довести усвідомлення ОСОБА-1 наслідків своїх дій, що може бути підтверджено її діями, заявами, планами або іншими доказами, що свідчать про те, що вона усвідомлювала наслідки для потерпілих.

Що стосується меж доказування у справі ОСОБА-2, то необхідно довести, що вона виконувала вказівки організатора. Це може бути підтверджено електронними повідомленнями, документами чи свідченнями, які демонструють, що вона отримувала інструкції і виконувала їх, не маючи значного розуміння ситуації або усвідомлення наслідків своїх дій. Докази, які підтверджують обмежене інформування ОСОБА-2 або контроль, шантаж з боку організатора, можуть слугувати підставою для зняття з неї відповідальності і визнання її потерпілою особою в контексті кіберексплуатації.

Аналізуючи викладене та конкретні приклади, вважаємо за доцільним запропонувати впровадити статтю «кіберексплуатація людини» у Кримінальний кодекс України, оскільки таке радикальне реагування з боку законодавчої гілки держави є потребою в контексті сучасних викликів, які виникають у зв'язку з розвитком цифрових технологій та використанням Інтернету, штучного інтелекту.

Окрім цього, обґрунтування необхідності включення такої статті у кримінальний кодекс полягає у тому, що

такий важіль забезпечить правову базу для визначення та покарання різноманітних форм кіберексплуатації, зокрема такої важливої і актуальної форми як торгівля людьми через мережу Інтернет. Це включає в себе не лише традиційні види кіберзлочинності, такі як кібершахрайство та онлайн-експлуатація, але й нові, еволюціонуючі загрози, наприклад, використання штучного інтелекту для маніпулювання користувачами, кібербулінгу та тиску через соціальні мережі. Також, підсилювати захист прав та свобод громадян у цифровому просторі.

Отже, включення статті «кіберексплуатація людини» у Кримінальний кодекс України є важливим кроком для забезпечення правопорядку та безпеки в оцифрованій державі, відображає необхідність адаптації законодавства до сучасних викликів та технологічних змін.

Тож, таке правопорушення необхідно криміналізувати та викласти у окремій статті Кримінального кодексу України.

Стаття..... Кіберексплуатація людини

1. Залучення, використання або контроль над особою за допомогою інформаційно-комунікаційних технологій та мереж з метою незаконного отримання вигоди або завдання шкоди особі, – караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або пробацийним наглядом на строк до трьох років, або обмеженням волі на строк до трьох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, – караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк.

3. Дії, передбачені частинами першою або другою цієї статті вчинені стосовно неповнолітньої чи недієздатної особи, особи похилого віку, – штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян та позбавленням волі на строк від трьох до п'яти років.

Примітка* Дії, що можуть бути визнані кіберексплуатацією, включають, але не обмежуються: а) Використання фальшивих профілів або сторінок у соціальних мережах для залучення осіб до незаконних дій; б) Поширення шахрайської інформації або запитів за допомогою електронної пошти, текстових повідомлень або інших комунікаційних засобів; в) Використання програмного забезпечення для злову паролів або отримання несанкціонованого доступу до комп'ютерних систем; г) Поширення, продаж або обмін особистою інформацією, отриманою шляхом кіберексплуатації, без згоди особи.

Висновки. Таким чином, у світлі зростаючої кількості випадків кіберексплуатації людини та її негативного впливу на суспільство, можна стверджувати, що запропонована стаття стане важливим інструментом для законодавчого закріплення цього виду кримінального правопорушення. Вона надасть відповідним правоохоронним органам ефективні механізми для протидії кіберексплуатації.

Варто підкреслити, що кіберексплуатація може мати серйозні наслідки для жертв, включаючи фінансові втрати, порушення приватності, психологічні травми та інші форми шкоди. Впровадження законодавчих норм, що регулюють кіберексплуатацію людини, сприятиме посиленню захисту прав та інтересів громадян у цифровому просторі, забезпечуючи їм більшу безпеку.

Правова кваліфікація злочинів, пов'язаних із кіберексплуатацією, є критично важливою для забезпечення ефективного реагування правоохоронних органів. Слід зазначити, що існуючі законодавчі норми часто не враховують специфічні ризики та наслідки, пов'язані з кіберексплуатацією, що ускладнює їх розслідування та покарання винних осіб. Це підкреслює необхідність розробки спеціалізованих правових механізмів для ефективної протидії даному виду злочинності в сучасному цифровому середовищі.

ЛІТЕРАТУРА

1. Кібербулінг: правові механізми реагування. Інститут масової інформації. URL: <https://imi.org.ua/monitorings/kiberbuling-pravovi-mehanizmu-reaktsii-37574> (дата звернення: 20.03.2025).
2. Котова В.В. Особливості розслідування торгівлі людьми в умовах воєнного стану. *Українська поліцейстика: теорія, законодавство, практика* : навч.-практ. журнал. 2022. № 1. С. 74.
3. Кримінальний кодекс України: Закон України від 01 вер. 2001р. №2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#n976> (дата звернення: 20.03.2025).
4. Науково-практичний коментар Кримінального кодексу України / Азаров Д.С. та ін. ; за ред. О.М. Джужі, А.В. Савченка, В.В. Чернея. 2-ге вид., перероб. і допов. Київ: Юрінком Інтер, 2018. 1104 с.
5. Рішення Європейського суду з прав людини від 11 лютого 2020 року у справі "BUTURUGA v. ROMANIA" URL: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-200842%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200842%22]}) (дата звернення: 20.03.2025).