УДК 347.122 (045)
DOI https://doi.org/10.24144/2307-3322.2024.85.1.52

БОРОТЬБА З ШАХРАЙСТВОМ В ОНЛАЙН-ТОРГІВЛІ: ВИКЛИКИ СЬОГОДЕННЯ

Троцюк Н.В.,
кандидат юридичних наук, доцент,
доцент кафедри цивільного права і процесу
юридичного факультету
Національного авіаційного університету
ORCID: 0000-0002-5943-8694
e-mail: nina.trotsiuk@npp.nau.edu.ua

Славіта Ю.В.,
здобувачка вищої освіти
другого (освітньо-наукового) рівня
e-mail: 6264263@stud.nau.edu.ua

Троцюк Н.В., Славіта Ю.В. Боротьба з шахрайством в онлайн-торгівлі: виклики сьогодення.
Метою дослідження є визначення та обґрунтування ефективних заходів для підвищення рівня захисту споживачів і зниження ризиків шахрайства в онлайн-торгівлі. У роботі досліджуються шляхи покращення існуючих правових норм і механізмів, аналізуються чинні прогалини в регулюванні, а також пропонуються рекомендації для посилення захисту прав споживачів у цифровому середовищі. Методи дослідження: у роботі використовуються методи порівняльного аналізу для зіставлення законодавчих ініціатив України з міжнародним досвідом у боротьбі з шахрайством в онлайн-торгівлі. Також застосовуються методи системного підходу для виявлення зв'язків між законодавчими нормами та їх реалізацією на практиці, а також методи емпіричного аналізу для оцінки ефективності правозастосування в цій сфері. Результати дослідження показують, що, попри існування певних законодавчих ініціатив, спрямованих на боротьбу з шахрайством в онлайн-торгівлі, їх ефективність залишається недостатньою через прогалини в правовому регулюванні та слабку правозастосовну практику. Виявлено, що основними проблемами є відсутність чітких механізмів контролю та недостатній рівень захисту прав споживачів. Аналіз міжнародного досвіду демонструє, що впровадження більш суворих санкцій та автоматизованих систем моніторингу може суттєво знизити рівень шахрайства. Обговорення показало, що боротьба з шахрайством в онлайн-торгівлі є одним з найактуальніших викликів сучасного цифрового ринку, а динамічний розвиток електронної комерції створює нові можливості для злочинної діяльності, що потребує адекватних та своєчасних заходів протидії. Хоча Україна має певні напрацювання в боротьбі з шахрайством в онлайн-торгівлі, існуючі механізми потребують суттєвого вдосконалення. Особливу увагу слід приділити узгодженню національного законодавства з міжнародними стандартами та кращими практиками, що дозволить підвищити рівень захисту споживачів. Також важливо активізувати правозастосовну діяльність, зокрема через навчання працівників правоохоронних органів і залучення новітніх технологій для моніторингу та попередження шахрайських дій. Впровадження запропонованих заходів може суттєво підвищити ефективність боротьби з шахрайством у цифровому середовищі України.

Ключові слова: онлайн-торгівля, шахрайство, захист споживачів, законодавчі ініціативи, правозастосовна практика, цифрове середовище.

Trotsiuk N.V., Slavita Y.V. Combating fraud in online commerce: challenges of today.
The purpose of the study is to identify and justify effective measures aimed at increasing the level of consumer protection and reducing the risks of fraud in online commerce. The paper explores ways to improve existing legal norms and mechanisms, analyzes existing gaps in regulation, and offers

recommendations for strengthening consumer protection in the digital environment. Research Methods: the paper uses comparative analysis methods to compare Ukraine's legislative initiatives with international experience in combating fraud in online commerce. Also, the methods of systematic approach are used to identify the links between legislative norms and their implementation in practice, as well as methods of empirical analysis to assess the effectiveness of law enforcement in this area. The results of the study show that, despite the existence of certain legislative initiatives aimed at combating fraud in online commerce, their effectiveness remains insufficient due to gaps in legal regulation and weak law enforcement practice. The main problems are the lack of clear control mechanisms and insufficient consumer protection. The analysis of international experience shows that the introduction of stricter sanctions and automated monitoring systems can significantly reduce the level of fraud. The discussion showed that the combat against fraud in online commerce is one of the most pressing challenges of the modern digital market, and the dynamic development of e-commerce creates new opportunities for criminal activity that requires adequate and timely countermeasures. Particular attention should be paid to harmonizing national legislation with international standards and best practices, which will increase the level of consumer protection. It is also important to intensify law enforcement activities, in particular through training of law enforcement officers and the use of the latest technologies to monitor and prevent fraud. Implementation of the proposed measures can significantly increase the effectiveness of the fight against fraud in the digital environment of Ukraine.

Key words: online commerce, fraud, consumer protection, legislative initiatives, law enforcement practice, digital environment.

Постановка проблеми. Інтернет-комерція сьогодні є невід'ємною частиною глобальної економіки. Проте, з розвитком технологій та зростанням популярності онлайн-торгівлі, спостерігається тенденція до збільшення кількості шахрайських дій, спрямованих на споживачів та продавців. Ці загрози, які раніше здавалися маргінальними, стали серйозною перешкодою для розвитку цифрової економіки. Враховуючи це, боротьба з шахрайством в онлайн-торгівлі набуває особливої актуальності.

Одним із головних факторів, що підвищують актуальність боротьби з шахрайством в онлайн-торгівлі є постійне зростання кількості шахрайських схем. Сьогодні злочинці використовують витончені технології та психологічні маніпуляції для досягнення своїх цілей. Фішинг, фармінг кардинг та інші види шахрайства стали звичними проблемами для користувачів в мережі Інтернет. В свою чергу, злочинці адаптуються до нових технологій та способів захисту, що робить їх виявлення та притягнення до відповідальності дедалі складнішим завданням.

Слід зазначити, що додатково ускладнює ситуацію в Україні транснаціональний характер шахрайства, адже шахраї можуть діяти з будь-якого куточка світу, що робить координацію міжнародних правоохоронних органів надзвичайно важливою, але водночас складною. Це також ускладнює процес відновлення справедливості для жертв шахрайства, оскільки законодавчі системи різних країн часто не узгоджені між собою.

Вразливість споживачів є ще одним важливим аспектом, який підкреслює актуальність проблеми. Багато користувачів не мають достатніх знань про безпеку онлайн-транзакцій, що робить їх легкою «мішенню» для шахраїв, а це у свою чергу створює додаткові ризики не лише для індивідуальних споживачів товарів та послуг, але й для загальної довіри до системи онлайн-торгівлі.

Значні фінансові втрати, які зазнають як окремі особи, так і бізнеси, є ще одним свідченням важливості боротьби з шахрайством, адже це підриває довіру до електронної комерції, що може мати довгострокові негативні наслідки для розвитку цифрової економіки. Тому для захисту прав споживачів і забезпечення стабільного розвитку цієї сфери, необхідно приймати рішучі заходи.

Законодавчі ініціативи та правозастосовна практика також відіграють ключову роль у боротьбі з шахрайством в онлайн-торгівлі. Вважаємо, що необхідно якнайшвидше розробити та впровадити нові законодавчі норми, які б відповідали сучасним викликам у сфері кібербезпеки.

І ще одним вирішальним питанням у боротьбі з шахрайством в онлайн-торгівлі є підвищення обізнаності населення про основи безпеки онлайн-транзакцій та розвиток технологій захисту, таких як системи виявлення шахрайства та інші інструменти кібербезпеки. Таким чином, інформаційні кампанії, що спрямовані на навчання користувачів мережі Інтернет, можуть допомогти зменшити кількість жертв шахраїв, що є не менш важливим елементом у боротьбі з цим видом злочинності.

Стан опрацювання проблематики. Проблема шахрайства в онлайн-торгівлі стала надзвичайно актуальною в сучасному світі, адже все більше людей здійснюють покупки через мережу Інтернет. Зростання кількості онлайн-транзакцій супроводжується збільшенням кількості спроб обману з боку недобросовісних продавців та покупців. Для ефективної боротьби з цим явищем необхідний комплексний підхід, який включає як законодавчі ініціативи, так і активну правозастосовну практику.

Аналіз існуючих досліджень показує, що проблема шахрайства в онлайн-торгівлі активно досліджується як в Україні, так і за кордоном. Дослідники зосереджуються на різних аспектах цього явища, включаючи типи шахрайства, законодавче регулювання, правозастосовну практику та роль технологій.

Проблеми у боротьбі з шахрайством в онлайн-торгівлі неодноразово привертали увагу наукової спільноти та працівників Департаменту кіберполіції Національної поліції України, а проведені дослідження в цій сфері охоплюють різноманітні підходи та методи. Наприклад, у публікаціях Сметанка О.В. [1] розглянуто удосконалення процесу внутрішнього аудиту причин шахрайства в системі корпоративного управління. Шапочка С.В. [2] досліджує боротьбу з шахрайством, що виникає через використання можливостей мережі Інтернет. Науковці Орлов Р.Р., Окушко А.В [3] окреслюють новели у сфері шахрайства з платіжними інструментами, а останні праці Чекмарьової І.М. присвячені розвитку шахрайства в Інтернеті на тлі сучасних подій в Україні [4]. Начальник відділу протидії різновидам онлайн-шахрайств Департаменту кіберполіції Національної поліції України Ульяненков О.В. у своїх публікаціях зазначає про необхідність створення бази дропів для боротьби з онлайн-шахрайством [5].

Таким чином, як бачимо боротьба з шахрайством в онлайн-торгівлі є складним і багатогранним процесом, що потребує злагодженої роботи на різних рівнях. Важливо продовжувати дослідження в цій області, вдосконалювати законодавство, посилювати правозастосовчу практику та використовувати сучасні технології для ефективного вирішення цієї проблеми.

Метою цього дослідження є визначення та обґрунтування ефективних заходів для підвищення рівня захисту прав споживачів і зниження ризиків шахрайства в онлайн-торгівлі. У роботі досліджуються шляхи покращення існуючих правових норм і механізмів, аналізуються чинні прогалини в правовому регулюванні захисту прав споживачів у цифровому середовищі, а також пропонуються окремі рекомендації.

Виклад основного матеріалу. Онлайн-шахрайство або кібершахрайство є однією з найбільших загроз сучасного цифрового суспільства. Це явище охоплює будь-які незаконні дії, що здійснюються через комп'ютерні системи або мережу Інтернет з метою завдання матеріальної шкоди чи отримання незаконного збагачення. Як у юридичному, так і в загальному розумінні, онлайн-шахрайство характеризується обманом та зловживанням довірою користувачів онлайн-середовища.

Основні види онлайн-шахрайства включають фішинг, фрод, соціальну інженерію, викуп даних, розповсюдження шкідливого програмного забезпечення та фальшиві онлайн-магазини. Фішинг є найпоширенішим видом шахрайства, що передбачає виманювання конфіденційної інформації, такої як логін, пароль чи номер банківської картки. Це здійснюється через підроблені листи, повідомлення або веб-сайти, що імітують легітимні джерела. Метою фішингу є отримання доступу до особистих даних жертви, що дозволяє зловмисникам здійснювати несанкціоновані фінансові операції.

Фрод, більш загальний термін, охоплює різноманітні фінансові махінації. Ним може бути кардинг, де викрадені банківські дані використовуються для несанкціонованих платежів або отримання кредитів за чужим паспортом через підроблені документи. На нашу думку, інвестиційні шахрайства представляють особливу загрозу, обманюючи інвесторів під приводом обіцяної високої прибутковості, що в кінцевому результаті призводить до заволодіння їхніми коштами.

До інших видів онлайн-шахрайства можна віднести соціальну інженерію, де шахраї маніпулюють людьми для отримання конфіденційної інформації та викуп даних (ransomware), де файли на комп'ютері жертви шифруються, а для їх розшифрування вимагається викуп. Розповсюдження шкідливого програмного забезпечення, яке може «красти» дані, контролювати системи або знищувати інформацію також є серйозною проблемою.

Окрему увагу заслуговують фальшиві онлайн-магазини, що створюються для збору платежів без подальшого надання товарів чи послуг.

Особливостями онлайн-шахрайства є анонімність злочинців, адже мережа Інтернет дозволяє приховувати свою особистість, використовуючи проксі-сервери, VPN та інші засоби анонімізації.

Транснаціональний характер цієї проблеми ускладнює розслідування та переслідування злочинців, оскільки шахрайські дії можуть здійснюватися з будь-якої точки світу. Швидкість з якою нові шахрайські схеми з'являються та поширюються додає складнощів у боротьбі з ними.

Належне законодавче регулювання цивільних правовідносин в зазначеній сфері є важливим аспектом у боротьбі з шахрайством в онлайн-торгівлі. Аналіз існуючих законів, що регулюють електронну комерцію, показує, що багато країн, включаючи Україну, мають певні норми, які намагаються боротися з цим явищем. Проте, часто виникають проблеми з їх ефективністю, оскільки технології швидко розвиваються, а суб'єкти законодавчої ініціативи не завжди встигають за цими змінами. Тому важливо постійно вдосконалювати законодавство, враховуючи нові сучасні виклики.

Серед основних документів, що регулюють дані відносини, варто виділити Цивільний кодекс України [6], Господарський кодекс України [7], Закон України «Про захист прав споживачів» [8], Закон України «Про електронну комерцію» [9], а також Закон України «Про захист персональних даних» [10].

Однак, незважаючи на існування значної кількості нормативних актів, українське законодавство щодо онлайн-торгівлі має свої прогалини. Наприклад, деякі положення законів є досить загальними та потребують більш детальної регламентації, особливо в контексті електронної комерції.

Варто зазначити, що на сьогодні існує ряд законодавчих ініціатив для вирішення вище зазначених проблем. Наприклад, Верховною Радою України прийнято за основу законопроєкт щодо встановлення відповідальності за електронно-комунікаційне шахрайство, який доповнює Кримінальний кодекс України (далі – КК) новими статтями 190^{1}, 255^{4}, 255^{5}. Вказаними нормами передбачається кримінальна відповідальність за:

– електронно-комунікаційне шахрайство, тобто протиправне збирання, зберігання, обробку та використання персональних даних, інформації, яка містить банківську таємницю, у тому числі індивідуальну облікову інформацію, реквізити платіжного інструменту, платіжної картки, код авторизації, з метою заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою з використанням електронної комунікації та/або технічних засобів електронних комунікацій (ст. 190^{1} КК);

– створення, керівництво електронно-комунікаційною шахрайською організацією, а також участь у ній (ст. 255^{4} КК);

– залучення до участі в електронно-комунікаційній шахрайській організації (ст. 255^{5} КК).

Даний законопроєкт спрямований на посилення боротьби з шахрайськими кол-центрами, які професійно займаються обманом громадян України. Зокрема, за створення, керівництво електронно-комунікаційною шахрайською організацією, а також участь у ній пропонується покарання від 7 до 12 років позбавлення волі з конфіскацією майна. Вважаємо, що прийняття даного законопроєкту сприятиме удосконаленню та посиленню кримінальної відповідальності за електронно-комунікаційне шахрайство та в результаті відбудеться зниження рівня злочинності у цій сфері [5].

Правозастосовна практика є ще одним важливим аспектом у боротьбі з шахрайством. Судові рішення та правоохоронна діяльність в справах про шахрайство в онлайн-торгівлі демонструють різний рівень ефективності в залежності від країни та юрисдикції. В Україні, наприклад, діяльність Національної поліції та інших органів правопорядку зосереджена на виявленні та розслідуванні таких злочинів, проте часто стикається з труднощами через недостатню технічну оснащеність та обмежені ресурси. Тому, на сьогодні важливу роль у запобіганні та розслідуванні шахрайських дій відіграють сучасні технології. Розвиток штучного інтелекту, машинного навчання та систем моніторингу транзакцій допомагають виявляти підозрілі дії та запобігати шахрайству, а технологічні компанії, що надають послуги в сфері електронної комерції разом з банками та платіжними системами постійно працюють над вдосконаленням своїх систем безпеки задля забезпечення захисту прав своїх користувачів.

Проблеми виникають також і в сфері доведення фактів у судовому порядку, що стосується укладення електронних договорів та здійснення електронних платежів. Водночас швидкий розвиток технологій вимагає постійного оновлення законодавства, щоб воно могло регулювати нові форми онлайн-торгівлі, такі як криптовалюта або смарт-контракти.

Україна, намагаючись гармонізувати своє законодавство з міжнародними стандартами в даній сфері приділяє увагу імплементації міжнародних директив та модельних законів, розробле-

них юридичним органом ООН в сфері міжнародної торгівлі (ЮНСІТРАЛ). Використання досвіду Європейського Союзу, навіть при відсутності членства, може допомогти в удосконаленні національного законодавства та сприятиме розвитку довіри до онлайн-торгівлі, що є важливим для економічного зростання нашої країни.

Вважаємо, що аналіз законодавчих ініціатив щодо боротьби з онлайн-шахрайством є ключовим аспектом для розуміння поточного стану правової системи та напрямків її подальшого розвитку. Розглядаючи ці ініціативи, важливо акцентувати увагу на кількох аспектах. По-перше, важливо визначити об'єкт регулювання, тобто, які конкретні види онлайн-шахрайства охоплюються законопроектами. Чи є чітке визначення ключових понять, таких як фішинг, скіммінг, або фальсифікація платіжних реквізитів? Чіткість у визначеннях допомагає уникнути правових прогалин і забезпечити ефективність заходів, що вживаються.

По-друге, необхідно встановити суб'єктів відповідальності. Суб'єкти законодавчої ініціативи повинні визначати, хто несе відповідальність за вчинення онлайн-шахрайства, включаючи не лише безпосередніх злочинців, але й платформи, через які відбувається злочин. Важливо також розглянути, які обов'язки покладаються на електронні майданчики, фінансові установи та інших учасників ринку, адже це дозволить чітко визначити, де лежить відповідальність за безпеку та захист прав споживачів.

Захист прав споживачів є третім критично важливим аспектом. Необхідно розглянути, які гарантії надаються споживачам, які стали жертвами онлайн-шахрайства та які механізми відшкодування збитків передбачені законопроектами. Це забезпечить реальну можливість для постраждалих отримати компенсацію та відновити свої права.

Створення спеціалізованих органів для боротьби з кіберзлочинністю є ще одним важливим кроком у даному напрямку. Спеціалізовані підрозділи в правоохоронних органах повинні займатися виключно боротьбою з кіберзлочинністю, забезпечувати ефективну міжвідомчу координацію та постійно підвищувати кваліфікацію фахівців. Слушно з даного приводу висловлюється начальник відділу протидії різновидам онлайн-шахрайств Департаменту кіберполіції Національної поліції України Олександр Ульяненков. Він пропонує Департаменту кіберполіції Національної поліції України разом з банками створити базу дропів для боротьби з онлайн-шахрайством (осіб, які використовуються шахраями для виводу коштів) з метою підвищення ефективності боротьби з онлайн-шахрайством. Дана ініціатива допоможе кіберполіції боротися з шахрайством в мережі Інтернет [11].

Не менш важливим питанням є також аналіз правозастосовної практики в справах про онлайн-шахрайство з метою розуміння сучасних викликів у сфері боротьби з кіберзлочинністю. Одним з основних етапів такого аналізу є вивчення статистики судових рішень, яка надає загальну картину про кількість розглянутих справ, їх категорії та масштаби економічної шкоди.

Вважаємо, що на сьогоднішній день глобальний характер онлайн-шахрайства визначається кількома ключовими факторами: 1) злочинці часто використовують інфраструктуру різних країн для реалізації своїх схем; 2) інформація про нові шахрайські методи поширюється в мережі дуже швидко, що ускладнює оперативну реакцію на загрози; 3) складність ідентифікації злочинців зумовлена використанням фальшивих імен, IP-адрес та інших методів маскування, що ускладнює їх затримання; 4) міжнародні фінансові потоки, через які шахраї переводять гроші роблять процес відстеження коштів надзвичайно складним.

Головна мета боротьби з шахрайством в онлайн-торгівлі повинна полягати в забезпеченні безпеки онлайн-транзакцій, зменшенні кількості шахрайських дій, підвищенні довіри до електронної комерції та захисті прав споживачів. Для досягнення цих цілей необхідно вжити комплексних заходів, включаючи удосконалення законодавства, посилення міжнародного співробітництва, підвищення обізнаності населення, розвиток технологій захисту та тісну співпрацю між бізнесом та державою.

Висновки. Боротьба з шахрайством в онлайн-торгівлі є одним з найактуальніших викликів сучасного цифрового ринку, а динамічний розвиток електронної комерції створює нові можливості для злочинної діяльності, що потребує адекватних та своєчасних заходів протидії.

Однією із проблем, яку необхідно якнайшвидше вирішити, є недостатність та розрізненість законодавчої бази, адже суб'єкти законодавчої ініціативи часто не встигають за швидкими темпами розвитку технологій та нових схем шахрайства. Складність ідентифікації та переслідування злочинців ще більше ускладнюється через високий рівень анонімності в мережі Інтернет. Вико-

ристання криптовалют та інших засобів маскування, таких як анонімізатори та фальшиві особистості, роблять розслідування шахрайських схем і притягнення винних до відповідальності особливо складним завданням.

Ще одним значним фактором є низький рівень кібергігієни користувачів, адже недостатня обізнаність споживачів про загрози в мережі Інтернет, а також відсутність навичок безпечної онлайн-діяльності роблять їх вразливими до шахрайських атак.

На нашу думку, для ефективного протистояння шахрайству в онлайн-торгівлі необхідно вжити комплексних заходів. Насамперед, слід посилити міжнародне співробітництво, оскільки створення ефективних механізмів обміну інформацією та координації дій між правоохоронними органами різних країн може значно покращити ситуацію. Також варто постійно удосконалювати національне законодавство та налагодити співпрацю державних органів, бізнесу та громадянського суспільства. Дана співпраця сприятиме обміну інформацією, розробленню спільних стратегій та координації дій для боротьби з шахрайством. Тільки комплексний підхід, що поєднує ці різні елементи, може забезпечити суттєве зменшення кількості шахрайських діянь в електронній комерції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Сметанко О.В. Удосконалення процесу внутрішнього аудиту причин шахрайства в системі корпоративного управління. *Економічний форум*. 2025. № 3. С. 424–430.
2. Шапочка С.В. До питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет. *Правова інформатика*. 2014. № 3 (43). С. 89–95.
3. Орлов Р.Р., Окушко А.В. Різновиди онлайн шахрайств та методи протидії злочинам у мережі Інтернет. Застосування інформаційних технологій у правоохоронній діяльності: *матеріали круглого столу*, м. Харків, 14 грудня 2023 р. Харків, 2023. С. 50–52.
4. Чекмарьова І.М. Шахрайство в Інтернеті як один із видів шахрайства. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 639–643.
5. В Україні можуть сформувати базу дропів для боротьби з онлайн-шахрайством. URL: https://cyberpolice.gov.ua/news/v-ukrayini-mozhut-sformuvaty-bazu-dropiv-dlya-borotby-z-onlajn-shaxrajstvom---kiberpolicziya-4292.
6. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV. *Відомості Верховної Ради України.* 2024. № 15–18. Ст. 74.
7. Господарський кодекс України: Закон України від 16.01.2003 р. № 436-IV. *Відомості Верховної Ради України.* 2021. № 46. Ст. 378.
8. Про захист прав споживачів: Закон України від 12.05.1991 р. № 1023-XII. *Відомості Верховної Ради України.* 2021. № 36. Ст. 310.
9. Про електронну комерцію: Закон України від 03.09.2015 р. № 675-XIII. *Відомості Верховної Ради України.* 2020. № 28. Ст. 188.
10. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України.* 2023. № 15. Ст. 52.
11. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за електронно-комунікаційне шахрайство. URL: https://zakon.rada.gov.ua/laws/show/3741-20#Text.