DOI https://doi.org/10.24144/2307-3322.2021.68.38
УДК 343.9

ДОСВІД ЗАПОБІГАННЯ ШАХРАЙСТВУ В СФЕРІ ЕЛЕКТРОННОЇ ТОРГІВЛІ В США

Коновалова І. О.,
аспірантка кафедри кримінології та кримінально-виконавчого права Національний юридичний університету імені Ярослава Мудрого

Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США.

У статті здійснено кримінологічний аналіз запобігання електронному торговельно-комерційному шахрайству в Сполучених Штатах Америки. Зазначено, що наукова площина досліджень сучасного шахрайства потребує постійного емпіричного оновлення і теоретичного осмислення в галузі кримінології та віктимології, зокрема, у частині дослідження шахрайства у сфері електронної комерції та торгівлі.

Основою наукового кримінологічного аналізу стало комплексне поєднання філософських (зокрема, діалектичний), загальнонаукових (синтез, аналіз, індукція, дедукція й узагальнення) та спеціально-наукових методів.

Для мети даної праці, зокрема, обґрунтовано особливості запобігання електронного торговельно-комерційного шахрайства в США, а саме: 1) описано норми спеціальних законів щодо запобігання онлайн-шахрайству у сфері електронної комерції та торгівлі; 2) визначено суб'єктів, які здійснюють роботу по запобіганню даного виду кримінальних правопорушень; та 3) розглянуто новітні технології, які використовуються у цій сфері. Особлива увага автора приділена формально-усталеним правилам захисту інтернет-магазинів США від різного роду загроз шахрайства, які покликані зменшити їх ризик у сфері електронної торгівлі та розглянуті важливі інструменти виявлення та запобігання шахрайству.

У висновках окреслені універсальні механізми ефективного запобігання кримінальним правопорушенням у даній сфері, вироблення яких надалі дозволить напрацювати концептуальні заходи державної політики щодо протидії шахрайствам; та створити програму дій для правоохоронних органів.

Ключові слова: шахрайство, шахрайство в електронній комерції та торгівлі, запобігання шахрайству, досвід США.

Konovalova I. O. Experience of prevention e-commercial fraud in the USA.

The article analyzes the prevention of electronic trade and commercial fraud in the United States of America. It is noted that the scientific area of research of modern fraud requires constant empirical updating and theoretical understanding in the field of Crivinology and Victimology, in particular, in the area of fraud research in the sphere of electronic commerce and trade.

The basis of the scientific Crimean-logical analysis was a complex combination of philosophical (in particular, dialectic), general scientific (synthesis, analysis, indouction, and generalization) and special-scientific methods.

For the purpose of this work, in particular, the peculiarities of prevention of electronic trade and commercial fraud in the USA are justified, namely: 1) the rules of special laws on prevention of online fraud in the sphere of electronic commerce and trade are described; 2) the subjects which carry out work on prevention of this type of criminal offense are defined; and 3) considered the latest technologies used in this field. Special attention is paid to the formal-established rules of protection of online shops of the USA from various kinds of threats of fraud, which are aimed at reducing their risk in the sphere of electronic trade and considered important tools of detection and prevention of fraud.

The conclusions set out universal mechanisms for effective prevention of criminal offenses in this sphere, the elaboration of which will further develop conceptual measures of state policy on counteraction to fraud; and create a program of action for law enforcement bodies.

Key words: fraud, fraud in electronic commerce and trade, fraud prevention, U.S. experience.

Постановка проблеми. Проблема злочинності має бути у центрі уваги правової держави, адже саме злочинність як складний феномен знецінює життя і безпеку кожної людини, руйнує економічне, соціальне підґрунтя нашої держави, її інформаційну безпеку, правовий порядок та духовність [1, с. 11]. Тоді як шахрайство у сфері електронної торгівлі – один із видів корисливої злочинності, системоутворюючою ознакою якого виступає спільна корислива мотивація до незаконного збагачення та спрямованість злочинної поведінки на заволодіння матеріальними благами у різний спосіб або отримання іншої незаконної вигоди [2, с. 17]; характеризується значною поширеністю, багатомільйонними збитками, організованим характером, а також складністю його виявлення та запобігання. У контексті глобальних змін економіки та банківського сектору, процесів діджиталізації суспільства, шахраї демонструють винахідливість, створюють витончені методи шахрайства, а їхні підходи швидко змінюються та адаптуються. Саме тому, особливий інтерес викликає досвід США щодо запобігання електронного комерційного шахрайства з метою розроблення універсальних механізмів ефективного запобігання кримінальним правопорушенням у даній сфері, вироблення яких надалі дозволить напрацювати концептуальні заходи державної політики щодо протидії шахрайствам; та створити програму дій для правоохоронних органів.

Стан опрацювання теоретико-методологічних засад запобігання різним видам економічного (фінансового) шахрайства висвітлювались у роботах багатьох вітчизняних та зарубіжних учених, зокрема: П. П. Андрушка, О. М. Бандурки, А. М. Бойка, В. В. Голіни, Б. М. Головкіна, А. П. Закалюка, А. Ф. Зелінського, О. Г. Кальмана, О. М. Костенка, П. М. Коваленко, Н. Ф. Кузнєцової, О. В. Лисодєда, А. В. Микитчика, А. А. Музики, І. А. Нестерової, В. Л. Пластуна, К. Л. Попова, В. Я. Тація та ін. Проте, не применшуючи значення та цінність робіт названих науковців, слід зазначити, що вказана тематика потребує постійного оновлення в галузі кримінології та віктимології, а саме: дослідження шахрайства у сфері електронної комерції та торгівлі.

Мета статті визначити основні напрями запобігання шахрайству у сфері електронної торгівлі в США.

Виклад основного матеріалу. Якщо 20 років тому телефони використовувалися лише для дзвінків, Google – для пошуку інформації, Facebook – для зв'язку з друзями, eBay – для збуту старих непотрібних речей, а Amazon був онлайн-магазином продажу книг, то у 2020-х рр. Amazon, Google і Facebook стали трьома «китами», на яких «тримається» електронна торгівля всього світу. Електронна комерція та торгівлі настільки глобалізувалися, що в результаті онлайн-магазини перетворилися у великі торговельні інтернет-площадки. Сьогодні найбільшим інтернет-ритейлером у світі є Amazon, на просторах якого можна придбати будь-що - від годинника до автомобіля; найбільшим інтернет-аукціоном - eBay, прибуток якого постійно зростає та вже перевищує 8,5 млрд дол. США; а Zappos.com – найбільший онлайн-магазин, заснований ще наприкінці 90-х рр. минулого століття (прибуток компанії перевищує 1 млрд дол.). Відповідні онлайн-площадки були засновані та продовжують свою діяльність в США.

Справедливо зауважити, що електронна торгівля займає провідне місце в економіці зарубіжних країн, особливо, в умовах запровадження соціальної дистанції, карантину та інших обмежувальних заходів в період пандемії COVID-19. Починаючи з 2019 р. по 2021 р. відбулося значне зростання електронної комерції як у сегменті B2C, так і в сегменті B2B. Доходи інтернет-магазинів США станом на 2020 рік збільшилися на 68 %, у порівнянні з аналогічним періодом минулого року [3], а кількість інтернет-замовлень у США та Канаді виросли у 2,5 раза [4]. У сегменті B2C дана тенденція відбивається серед продажу предметів медичного призначення, предметів першої необхідності, продуктів харчування, електроніки та т. і.

Процвітання світової електронної комерції та електронної торгівлі призводить до збільшення кількості шахрайств у даній сфері. Говорячи комерційною мовою: попит породжує пропозицію. Так, у США у 2020 р. загальний обсяг транскордонного шахрайства склав 33968 випадків, із заявленими збитками у розмірі 91,95 млн дол. США, у порівнянні з 14 797 заявами та зі збитками, у розмірі 40,83 млн дол. США, 5 років тому. Ці скарги включали шахрайство при покупках в Інтернеті, спотворення інформації про товари, випадки, коли товари не були доставлені, та проблеми із поверненням коштів. Сполучені Штати посіли перше місце серед десяти країн з розвиненою електронною торгівлею за кількістю поданих заяв та скарг на шахрайство в мережі Інтернет [5].

Як наслідок цього, міжнародне співтовариство занепокоєне поширенням та ростом шахрайств у електронній торгівельно-комерційній сфері, адже збитки від даного виду кримінальних правопорушень завдають шкоди не тільки продавцям та споживачам, а й економікам цілих країн. Тому, нижче на прикладі США розглянемо найкращі практики запобігання шахрайству в сфері електронної торгівлі, звернемо увагу на наявність спеціальних законів та суб'єктів, які здійснюють роботу по запобіганню онлайн-шахарайствам, а також розглянемо новітні технології, що використовуються у даній сфері.

Перш за все варто зазначити, що в англомовних країнах існує термін *ecommerce fraud*, який перекладається як шахрайство у сфері електронної торгівлі. Відповідно до визначення BigCommerce – однієї з найбіль-

ших платформ електронної комерції, діяльність якої направлена на створення інтернет-магазинів, оптимізацію пошукових систем, хостинг, маркетинг та безпеку від малого до великого бізнесу; *ecommerce fraud* – це злочинний обман, що здійснюється під час комерційної транзакції через Інтернет з метою отримання фінансової або іншої особистої вигоди шахрая, негативно впливаючи на чистий прибуток продавця [6].

Перш ніж перейти до заходів запобігання ecommerce fraud, звернемося до нормативної бази та безпосередньо суб'єктів такого запобігання в США. Так, у 1986 р. Конгресом був прийнятий спеціальний нормативний акт - *Computer Fraud and Abuse Act* (*Закон про комп'ютерне шахрайство та зловживання*), який заборонив будь-кому доступ до комп'ютера або комп'ютерної мережі без згоди власника [7]. Закон встановив кримінальну відповідальність за злом та крадіжку в мережі, знищення приватної або секретної інформації, а також за заволодіння чужим майном через комп'ютер. Після численних поправок до закону нормативний акт криміналізує навіть просту загрозу пошкодження комп'ютерного обладнання іншої людини, крадіжку комп'ютерних даних, публічне розповсюдження вкрадених даних та відмову виправити шкоду, заподіяну злочинцем комп'ютеру жертви, наприклад, за допомогою програм-вимагачів. Пізніше, у 2003 році Конгрес прийняв *Controlling the Assault of Non-Solicited Pornography and Marketing Act*, більш відомий як *Закон про CAN-SPAM*, який забороняє використовувати в електронних листах помилкові або ті, що вводять в оману, тематичні заголовки, тема листа повинна бути точною, а повідомлення – чітко визначені [8]. Ще одним важливим нормативно-правовим актом США, який забезпечує захист прав споживачів в Інтернеті, є *Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act* 2006 року, більш відомий як *Закон про безпеку в Інтернеті*. Основна мета SAFE WEB – боротьба зі спамом, інтернет-шахрайством та обманом. У той час, як інші законодавчі акти були зосереджені, у першу чергу, на боротьбі з кібершахрайством на національному рівні, то у Законі про безпеку в Інтернеті основна увага приділена глобальним масштабам шахрайства. У SAFE WEB передбачені важливі заходи захисту користувачів від спаму та інших інтернет-атак, з цією метою розширено повноваження Федеральної торговельної комісії (FTC) по боротьбі з міжнародним комп'ютерним шахрайством. Так, Закон про безпеку в Інтернеті дозволяє Федеральній торговельній комісії передавати свої конфіденційні дані закордонним правоохоронним органам, що дозволяє агентствам активно співпрацювати з іноземними колегами. Відповідне співробітництво дає змогу повноцінно контролювати міжнародну незаконну діяльність та спонукає інші держави до обміну взаємною інформацією [9].

Суб'єктами ж запобігання шахрайству у сфері електронної торгівлі в США є *Федеративне бюро (FBI)* та *Секретна служба США (United States Secret Service)*. На офіційному сайті ФБР визначено основну мету органу, яка полягає в тому, щоб змінити намір і поведінку злочинців та держав, які сподіваються зламати мережі США, вкрасти фінансову або інтелектуальну власність та поставити під загрозу іншу інфраструктуру, не наражаючи себе на ризик. ФБР – це провідне федеральне агентство з розслідування кібератак та інших злочинних вторгнень, структурними одиницями якого є спеціально обучені кібер-групи, які працюють по всій країні. Так, група швидкого реагування (Cyber Action Team) може розвернутися по всій країні протягом декілька годин, у разі серйозних інцидентів, а Центр скарг щодо Інтернет-злочинів (ІСЗ) збирає повідомлення від громадян [10]. У той час, основною метою Секретної служби США є захист фінансової інфраструктури країни та підтримка безпечних умов, у яких американський народ зможе проводити фінансові операції, а місією - розслідування складних фінансових злочинів в кіберпросторі. Для покращення роботи Секретною службою була створена Цільова група з кібершахрайства (CFTF), яка виступає основним центром з розслідування випадків шахрайства в мережі Інтернет, співпрацюючи з іншими правоохоронними органами, прокуратурою, приватним сектором та науковими колами. Стратегічна робота CFTF в боротьбі з кіберзлочинністю полягає в запобіганні, виявленні, розслідуванні злочинів та зменшенні заподіяної ними шкоди [11].

У результаті спільної роботи правоохоронних органів, представників електронного бізнесу, громадськості та науковців у США були формально створені усталені правила захисту інтернет-магазинів від різних видів шахрайств, які полягають у вживанні превентивних заходів та знижують ризик шахрайства у сфері електронної торгівлі. Розглянемо їх нижче.

1. *Регулярний аудит безпеки сайту* щодо: 1) оновлення програм для кошика покупок; 2) актуальності та дієвості роботи сертифіката SSL; 3) відповідності магазину стандарту безпеки даних індустрії платіжних карток - PCI-DSS; 4) наявності резервної копії магазину; 5) надійності паролів для облікових записів адміністраторів, панелей керування хостингом, бази даних та доступу по FTP; 6) сканування веб-сайту на наявність шкідливих програм та ін.
2. *Відповідність онлайн-магазину стандарту PCI DSS*. Інтернет-магазин, який приймає платежі за кредитними картками, повинен відповідати вимогам PCI DSS - стандарту безпеки даних індустрії платіжних карток, розроблений Радою зі стандартів безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council, PCI SSC), заснованою міжнародними платіжними системами Visa,

MasterCard, American Express, JCB та Discover. Стандарт являє собою сукупність 12 деталізованих вимог щодо забезпечення безпеки даних про власників платіжних карток, які передаються, зберігаються та обробляються в інформаційних інфраструктурах організацій. Прийняття відповідних заходів щодо забезпечення відповідності вимогам стандарту представляє комплексний підхід до забезпечення інформаційної безпеки даних платіжних карток [12].

3. *Регулярна перевірка сайту щодо підозрілої активності.* У зарубіжних країнах склалася практика, що онлайн-магазини наймають співробітників для запобігання шахрайству. Захистити інтернет-магазин від шахрайських транзакцій можна завдяки активному відстежуванню підозрілої активності, а саме: крадіжки персональних даних або взлому акаунту.
4. *икористання служби перевірки адрес (AVS).* AVS перевіряє: чи вказана клієнтом адреса виставлення рахунку відповідає самій адресі рахунку власника кредитної картки. Зазвичай автентифікація AVS використовується як частина багатошарової системи захисту від шахрайства, з метою гарантування затвердження дійсних транзакцій та відхилення тих, які вважаються підозрілими.
5. *Використання кодів CVV2, CVC2* - захисного коду платіжних карток, який закодований у магнітній смузі. Цей код потрібний для того, щоб банк міг ідентифікувати клієнта при оплаті товарів та послуг карткою онлайн та офлайн.
6. *Використання безпечного протоколу передачі гіпертексту (HTTPS)* - протоколу, який забезпечує цілісність та конфіденційність даних при їх передачі між сайтом та пристроєм користувача, який передбачає три основні рівні захисту: 1) шифрування переданих даних; 2) цілісність даних; та 3) аутентифікацію, яка гарантує, що відвідувачі потраплять саме на сайт, який їм потрібен, окрім цього, захищає від атаки посередника.
7. *Зберігання обмеженої кількості інформації*. Один зі способів захистити онлайн-магазин від витоку даних чи злому — зберігати якомога менше даних про клієнтів, адже, хакери не можуть вкрасти те, чого немає. Тому онлайн-магазинам рекомендується збирати та зберігати лише дані, необхідні для завершення транзакції та відправлення продукту, при цьому уникати збирання номерів соціального страхування, дат народження та інших непотрібних конфіденційних даних клієнтів.
8. *Встановлення обмеження* на кількість покупок та їх загальну вартість, які онлайн-магазин приймає з одного облікового запису протягом одного дня.
9. *Перевірки чи збігаються IP-адреса* (рядок чисел, розділених крапками, який ідентифікує кожен комп'ютер, який використовує Інтернет-протокол для зв'язку через Інтернет) *та адреса кредитної картки*. Кожне замовлення, розміщене в інтернет-магазині, надходить з унікальної загальнодоступної IP-адреси. За IP-адресую, зазвичай, можна визначити місто чи регіон світу де споживач здійснює покупку. Якщо це місто чи регіон не збігається з адресую кредитної картки, яка використовується, це може означати загрозу шахрайству.
10. *Використання програм для боротьби з шахрайством.* Коли справа доходить до виявлення та запобігання шахрайству в електронній торгівлі, існує безліч програмних рішень, які відповідають різним потребам та бюджету. Прості програми боротьби з шахрайством виконують специфічну функцію. Зазвичай, вони інтегровані в онлайн-кошики та платформи електронної комерції. Ці інструменти використовують алгоритми машинного навчання для виявлення шахрайських транзакцій за допомогою геолокації IP, перевірки адрес електронної пошти, проведення відбитків пальців пристрою та перевірки адрес. Програми для боротьби з шахрайством середнього рівня пропонують більш широкий спектр функцій, включаючи гарантії повернення платежів, автоматичне відхилення замовлень із високим ризиком, захист від нових шахрайств з обліковими записами та захист від поглинання облікового запису. Програми найвищого рівня захисту виконують всі ті ж функції, що й вищезазначені програми, а також пропонують аутсорсингове управління справами, роботу з великими продавцями, управління шахрайством із лояльністю, захист від зловживання політикою, автоматичне прийняття рішень та ручний перегляд підозрілих транзакцій, гарантуючи, що жодне хороше замовлення не буде помилково відхилено програмним забезпеченням. З даного питання, журнал Merchant Fraud склали список кращих платформ для запобігання шахрайству. Серед них: Kount, Riskified, Forter, Signifyd, ClearSale, CyberSource, Feedzai, Ravelin, Sift, Fraud.net, Nethone, Precognitive, SEON, FraudLabs Pro [13]. Відповідні програми при оплаті автоматизують перевірки на шахрайство, здійснюють блокування підозрілих пристроїв, скасування шахрайських замовлень та багато іншого.

Висновки. Отже, використання електронних систем запобігання шахрайству, а також електронних засобів контролю в США на сьогодні є пріоритетом та складовою міжнародної політики із ведення електронної комерційної діяльності.

На прикладі США виділимо першочергові завдання запобігання електронному комерційно-торгівельному шахрайству в Україні: 1) створення Єдиної інформаційної системи профілактики шахрайства у сфері електронної комерції та торгівлі, яка поєднуватиме різноманітні інформаційні ресурси, платформи та бази даних про шахраїв; 2) запровадження політики належного корпоративного управління; 3) упровадження дієвих законодавчих ініціатив щодо належного регулювання комерційної реклами та / або просування комерційних продуктів або послуг; встановлення кримінальної відповідальності за злом та крадіжку в мережі, знищення приватної та / або секретної інформації; 4) реформування інституту кримінальної відповідальності за електронне торговельно-комерційне шахрайство; 5) використання новітніх електронних систем та досягнень штучного інтелекту щодо запобігання електронного комерційного шахрайства; 6) популяризації електронної комерції через он-лайн та оф-лайн магазини; 7) посилення міжнародного співробітництва та залучення громадськості до соціально-виховної роботи з профілактики шахрайства в сфері електронної торгівлі.

Список використаних джерел:

1. Сметаніна Н. В. Наукові підходи до теорії злочинності у сучасній українській кримінології : монографія / за заг. ред. В. В. Голіни. Харків : Право, 2016. 192 с.

2. Головкін Б. М. Види злочинності. *Журнал східноєвропейського права*. 2015. №. 18. С. 14 – 21. URL: http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf (дата звернення: 15.12.2021).

3. Улучшение бизнес-результатов за счет отраслевой аналитики и сценариев использования, встроенных в платформу. URL: https://ccinsight.org/observations/us-retailers-see-online-growth-yoy-in-april-similar-to-recent-holiday-season/ (дата звернення: 04.11.2021).

4. Дані Forbs. URL: https://www.forbes.com/sites/louiscolumbus/2020/04/28/how-covid-19-is-transforming-ecommerce/#782a5edd3544 (дата звернення: 05.11.2021).

5. E-Commerce and Consumer Protection in India. *Journal of Business Ethics*, 2021. URL: https://link.springer.com/article/10.1007/s10551-021-04884-3 (дата звернення: 16.11.2021).

6. Global Ecommerce Update 2021 – eMarketer. URL: https://www.emarketer.com/content/global-ecommerce-update-2021 (дата звернення: 11.11.2021).

7. U.S. Code § 1030 - Fraud and related activity in connection with computers. URL: https://www.law.cornell.edu/uscode/text/18/1030#a_4 (дата звернення: 17.11.2021).

8. Закон о CAN-SPAM: Руководство по соответствию для бизнеса, Фед. Trade Comm. URL: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business (дата звернення: 17.11.2021).

9. Краткое изложение Закона США о безопасности в Интернете , Fed. Trade Comm. URL: Https://www.ftc.gov/sites/default/files/documents/reports/us-safe-web-act-protecting-consumers-spam-spyware-and-fraud-legislative-recommendation-congress/ summary-us-safe-web-act.pdf (дата звернення: 24.11.2021).

10. Cyber Crime — FBI. URL: https://www.fbi.gov/investigate/cyber (дата звернення: 24.11.2021).

11. United States Secret Service. URL: https://www.secretservice.gov/about/overview# (дата звернення: 24.11.2021).

12. PCI DSS – Вікіпедія. URL: https://uk.wikipedia.org/wiki/PCI_DSS (дата звернення: 26.11.2021).

13. Merchant Fraud Journal: eCommerce Fraud News Publication. URL: https://www.merchantfraudjournal.com/top-ecommerce-fraud-protection-solutions/ (дата звернення: 29.11.2021).