НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЯРОСЛАВА МУДРОГО
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

КОНОВАЛОВА ІЛОНА ОЛЕКСАНДРІВНА

УДК: 343.9:343.71:658.87

ДИСЕРТАЦІЯ
ЗАПОБІГАННЯ ШАХРАЙСТВУ У СФЕРІ ЕЛЕКТРОННОЇ ТОРГІВЛІ

081 «Право»

08 «Право»

Подається на здобуття наукового ступеня доктора філософії.

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ І. О. Коновалова

Науковий керівник:
Сметаніна Наталія Володимирівна,
кандидат юридичних наук, доцент.

Харків - 2023

АНОТАЦІЯ

Коновалова І. О. Запобігання шахрайству у сфері електронної торгівлі. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». – Національний юридичний університет імені Ярослава Мудрого, Міністерство освіти і науки України. – Харків, 2023.

Дисертація присвячена розробленню теоретичних і практичних засад запобігання шахрайству у сфері електронної торгівлі на основі результатів дослідження стану цього явища, криміногенних рис правопорушників, визначення й розкриття його детермінант, причин і умов, що зумовлюють кримінальні правопорушення.

У дисертації розглянуто генезис феномену шахрайства від часів Київської Русі до сьогодення. Наголошено, що під впливом глибинного проникнення цифрових та інноваційних технологій до бізнес-процесів, державного сектору, комунікацій, переходу економіки до ери цифрових можливостей шахрайство почало трансформуватися та набувати нових форм. Визначено основні кримінологічно важливі ознаки сучасного шахрая. Наголошено, що традиційне шахрайство зосереджується на особистому контакті шахрая й жертви, у той час, як електронне комерційне – на способі посягань. Незмінним залишається корисливий мотив, бажання отримати те, що не належить шахраю по праву.

Розкрито стан наукових досліджень проблем запобігання шахрайству у сфері електронної торгівлі. Констатовано, що наукова площина досліджень сучасного шахрайства з позицій кримінології потребує постійного емпіричного оновлення й теоретичного осмислення, зокрема, в частині вивчення шахрайства у сфері електронної комерції та торгівлі.

Розглянуто організаційні й правові засади функціонування електронної торгівлі в Україні. Констатовано, що в результаті триваючої цифровізації сучасного життя, підсиленої коронавірусною кризою COVID-19, стався зсув

попиту споживачів зі звичайної (традиційної, офлайн) торгівлі до електронної. Зроблено проміжні висновки, що прискорення науково-технічного прогресу зумовлює розвиток злочинного світу, призводячи до появи нових форм і видів шахрайства у сфері електронної торгівлі. Розкрито поняття «шахрайство у сфері електронної торгівлі» та надано перелік його істотних ознак, а саме: 1) глобальний характер; 2) вчинення кримінального правопорушення у кіберпросторі; 3) висока латентність та інші.

Зроблено спробу встановити й проаналізувати загальні кількісні та якісні характеристики сучасного шахрайства у сфері електронної торгівлі. При оцінці фактичного рівня злочинності враховано показники латентності. У цілому дослідження стану шахрайств у сфері електронної торгівлі підтвердило його негативну динаміку під час пандемії COVID-19, починаючи з 2019 по 2021 рр. Встановлено основні способи (форми) вчинення шахрайства у сфері електронної торгівлі, категорії товарів і послуг електронної комерції, якими «псевдопродавці-шахраї» зацікавлюють жертв, основні майданчики (майданчики), на яких вчиняється дане кримінальне правопорушення. На прикладі доведено, що для кримінологічної характеристики досліджуваного кримінального правопорушення час і місце вчинення злочину не мають значення.

Аргументовано, що шахрайство у сфері електронної торгівлі зумовлене наявністю комплексу причин, серед яких соціально-економічні, організаційно-управлінські й морально-психологічні чинники, система яких сформована, проведено їх аналіз. Зроблено висновок, що наведені та інші чинники тісно взаємопов’язані між собою і за кожним із них стоїть певне соціальне явище або проблема.

Здійснено кримінологічний, віктимологічний та психологічний аналіз взаємодії шахрая і жертви в електронному комерційному шахрайстві. Виокремлено особливості такого шахрайства. Так, контакт між шахраєм і жертвою встановлюється віддалено, дистанційно; цільова аудиторія шахрая з

огляду на використання цифрових технологій значно розширилася. Окреслено специфічні віктимні риси жертв електронного комерційного шахрайства, способи й прийоми, які використовують шахраї для побудови взаємодії з жертвою під час вчинення кримінального правопорушення. Статистично обґрунтовано, що ймовірність стати жертвою шахрайства у сфері електронної торгівлі значно підвищується у жадібних і надто довірливих осіб. Окремо розглянуто категорію азартних і самовпевнених жертв такого шахрайства, які характеризуються ризикованістю, вірять у щасливий випадок, при цьому мають гарну освіту, ведуть активний спосіб життя, пізнають нові види діяльності.

Проаналізовано особливості запобігання електронному комерційному шахрайству в зарубіжних країнах на прикладі світових лідерів електронної торгівлі – США і Китаю, а саме: 1) описано норми спеціальних законів щодо запобігання онлайн-шахрайству у сфері електронної комерції та торгівлі; 2) визначено суб'єктів, які провадять роботу з запобігання даному виду кримінальних правопорушень; 3) розглянуто новітні технології, які використовуються у цій сфері. Особлива увага приділена формально усталеним правилам захисту суб'єктів, які провадять електронну торговельно-комерційну діяльність, від різного роду загроз шахрайства, які покликані зменшити їх ризик у сфері електронної торгівлі. Розглянуто важливі інструменти виявлення й запобігання шахрайству. Окреслено універсальні механізми ефективного запобігання кримінальним правопорушенням у відповідній сфері.

Сформульовано положення про те, що загальносоціальне запобігання шахрайствам у сфері електронної торгівлі спрямовується на:

1. зниження рівня бідності й економічної депривації в суспільстві;
2. створення умов для реального збільшення доходів населення України;
3. розроблення стратегії зменшення рівня безробіття;

4. ведення ефективної культурно-виховної та просвітницької роботи серед споживачів товарів і послуг у сфері електронної торгівлі.

Спеціально-кримінологічне запобігання шахрайству у сфері електронної торгівлі охоплює заходи профілактики, відвернення і припинення кримінальних правопорушень. Зважаючи на те, що фізичне місцезнаходження шахрая, як і засобів учинення злочину, переважно не збігається з місцем перебування потерпілого й настанням негативних наслідків злочину (місцем завдання матеріальної шкоди), а за певних випадків такі обставини можуть мати навіть транснаціональний (трансконтинентальний) характер, зроблено висновок, що особливу увагу серед заходів спеціально-кримінологічного запобігання шахрайству у сфері електронної торгівлі варто приділити кримінологічній профілактиці.

До заходів профілактики віднесено:

1. формування цілісної нормативно-правової бази у сфері забезпечення кібербезпеки й боротьби з кіберзлочинністю, узгодження правових приписів законів і підзаконних нормативно-правових актів;
2. вдосконалення профільного законодавства у сфері електронної торгівлі;
3. розвиток співпраці з питань кібербезпеки правоохоронних органів, підприємств, установ, організацій всіх форм власності, засобів масової інформації (далі – ЗМІ);
4. контроль і облік осіб, які схильні до вчинення електронного комерційного шахрайства.

Розглянуто суб’єктів запобігання шахрайству у сфері електронної торгівлі й здійснено їх класифікацію. Вказано, що існуюча система суб’єктів запобігання електронному комерційному шахрайству не є досконалою. Звернено увагу на необхідність створення спеціального органу запобігання досліджуваному кримінального правопорушення і формування налагодженої співпраці між уже існуючими суб’єктами запобігання шахрайству у сфері електронної торгівлі.

Ключові слова: кримінальне правопорушення, шахрайство, електронна торгівля, шахрайство у сфері електронної торгівлі, причини та умови, запобігання.

SUMMARY

Konovalova I. O. *Prevention of Fraud in Electronic Commerce* – Qualification scientific work as a manuscript.

Thesis for obtaining a Doctor of Philosophy degree in specialty 081 "Law" – Yaroslav Mudry National Law University, Ministry of Education and Science of Ukraine – Kharkiv, 2023.

The dissertation is dedicated to developing the theoretical and practical foundations for preventing fraud in the sphere of electronic commerce based on the results of researching the state of this phenomenon, the criminogenic characteristics of offenders, defining, and revealing its determinants, causes, and conditions that lead to criminal offenses.

The dissertation examines the genesis of the fraud phenomenon from the times of Kyivan Rus to the present day. It emphasizes that due to the deep penetration of digital and innovative technologies into business processes, the public sector, communications, and the transition of the economy to the era of digital opportunities, fraud began to transform and take on new forms. The main criminologically significant features of the modern fraudster have been identified. It's emphasized that traditional fraud focuses on the personal contact between the fraudster and the victim, while electronic commercial fraud focuses on the method of intrusion. The selfish motive remains constant – the desire to obtain what does not rightfully belong to the fraudster.

The current state of scientific research into the prevention of fraud in electronic commerce has been revealed. It is acknowledged that the scientific landscape in the study of contemporary fraud from criminological perspectives

requires ongoing empirical updating and theoretical interpretation, particularly regarding the investigation of fraud in electronic commerce and trade.

The organizational and legal frameworks of electronic commerce in Ukraine have been thoroughly examined. It is evident that the continuous digitalization of contemporary life, compounded by the COVID-19 crisis, has led to a shift in consumer demand from traditional offline trade to electronic commerce. Preliminary conclusions highlight that the rapid advancement of scientific and technological progress is propelling criminal activities, resulting in the emergence of new forms and types of fraud within the realm of electronic commerce.

The concept of "fraud in electronic commerce" has been clearly defined, outlining a list of essential characteristics, such as: 1) its global nature; 2) the commission of criminal offenses in cyberspace; 3) high latency, and more. An endeavor has been made to establish and analyze the general quantitative and qualitative features of contemporary fraud in electronic commerce. The assessment of the actual crime level has taken latency indicators into account. Overall, the study of fraud in electronic commerce has validated its negative dynamics during the COVID-19 pandemic spanning from 2019 to 2021.

The primary methods (forms) of committing fraud in electronic commerce, categories of goods and services in e-commerce utilized by pseudo-vendors (fraudsters) to attract victims, and the primary platforms where these criminal offenses occur have been identified. Using specific examples, it has been demonstrated that, for the criminological characterization of the investigated criminal offense, the time and place of the crime are insignificant.

It is argued that fraud in electronic commerce is provoked by a complex set of reasons, including socio-economic, organizational-administrative, and moral-psychological factors. An analysis of these factors, along with their systemic formation, has been conducted. The drawn conclusion asserts that these and other

factors are interrelated, with each being associated with a specific social phenomenon or problem.

A detailed criminological, victimological, and psychological analysis of the interaction between the fraudster and the victim in electronic commercial fraud has been undertaken. Distinctive features of such fraud have been brought to light. For instance, the contact between the fraudster and the victim is typically remote and established over a distance. Furthermore, the fraudster's target audience has significantly broadened due to the pervasive use of digital technologies.

Specific victimological traits of those affected by electronic commercial fraud have been delineated, along with the strategies and approaches employed by fraudsters during the commission of criminal offenses. Statistical evidence has convincingly shown that the likelihood of falling victim to fraud in the realm of electronic commerce is markedly higher among both avaricious and overly trusting individuals. Moreover, a separate examination has been conducted on a particular category of daring and self-assured victims of such fraud. These individuals are characterized by their propensity for risk-taking behavior, a steadfast belief in fortuitous outcomes, high educational attainment, an active lifestyle, and a penchant for exploring novel activities.

The intricacies of preventing electronic commercial fraud in foreign countries have been scrutinized, focusing particularly on the leading global players in electronic commerce - the USA and China. This involved:

1. Describing specialized laws and regulations designed to prevent online fraud in electronic commerce and trade.
2. Identifying the entities actively involved in combatting this form of criminal offense.
3. Delving into the innovative technologies employed within this domain.

Special emphasis has been placed on established regulations aimed at safeguarding entities involved in electronic commerce from a spectrum of fraud risks, intending to mitigate their vulnerabilities within this realm. Vital methodologies for detecting and thwarting fraud have been deliberated upon, accompanied by universally applicable mechanisms for preventing criminal activities within this specific domain.

The stipulation posited underscores that the broader social measures to prevent fraud in electronic commerce aim at:

1. Reducing poverty levels and economic disparity within society.
2. Fostering an environment conducive to actual increases in the income of Ukraine's populace.
3. Developing strategies to alleviate the unemployment rate.
4. Carrying out effective cultural, educational, and awareness-raising initiatives among consumers of goods and services in electronic commerce.

Specialized criminological prevention against fraud in electronic commerce encompasses strategies for averting, deterring, and halting criminal offenses. It's highlighted that the physical location of fraudsters and the means of committing the crime seldom align with the victim's location and the resultant negative consequences (where material harm is inflicted). In some instances, these circumstances may even hold a transnational (transcontinental) character. The conclusion drawn is that among the methods of specialized criminological prevention in the field of electronic commerce, special attention should be directed towards criminological prevention.

The preventive measures encompass:

1. Establishing a comprehensive legal framework to ensure cybersecurity and combat cybercrime, aligning legal provisions in laws and subordinate legislative acts.

2. Enhancing specialized legislation within the electronic commerce domain.
3. Fostering collaborative efforts on cybersecurity among law enforcement agencies, enterprises, institutions, organizations of all ownership forms, and the mass media.
4. Monitoring and maintaining a record of individuals inclined towards engaging in electronic commercial fraud.

Subjects for the prevention of fraud in electronic commerce were studied and classified. It was noted that the current system of entities to prevent electronic commercial fraud is imperfect. The necessity of establishing a specialized body to prevent the investigated criminal offense and structuring well-coordinated cooperation among the existing subjects for preventing fraud in electronic commerce has been emphasized.

Keywords: criminal offense, fraud, electronic commerce, fraud in electronic commerce, causes and conditions, prevention.

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дослідження

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1) Коновалова І. О. Шахрайство і діджиталізація: історико-правовий аналіз. *Право і суспільство.* 2021. Вип. 3. С. 105-113.

2) Коновалова І. О. Жертва в електронному торговельно-комерційному шахрайстві. *Науковий вісник Ужгородського національного університету.* Серія : Право. Ужгород, 2021. № 65. С. 266-271.

3) Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. *Науковий вісник Ужгородського національного університету.* Серія : Право. Ужгород, 2021. № 68 (6). С. 220-225.

4) Коновалова І. О. Кримінологічна характеристика сучасного стану шахрайства у сфері електронної торгівлі. *Recht der Osteuropäischen Staaten.* 2022. № 1. С. 11-18.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

5) Коновалова І. О. До питання шахрайств у сфері електронної торгівлі. *Протидія організованій злочинності і корупції : матеріали XIX Всеукр. наук. конф. з кримінології для студентів, аспірантів та молодих вчених* (м. Харків, 2 груд. 2019 р.). Харків : Право, 2019. С. 69-71.

6) Konovalova Ilona. Modern forms of fraud. *Сучасне суспільство і наука: актуальні дослідження молодих науковців : матеріали Всеукр. наук.-практ. інтернет-конф. іноземними мовами*., (Харків, 29 травня 2020 р.). Харків : НЮУ ім. Ярослава Мудрого, 2020. С. 56-58.

7) Коновалова І. О., Пивоваров В. В. Шахрайство в умовах діджиталізації суспільства. *Діджиталізація і безпека : матеріали Міжнар. наук.-практ. конф*., (Харків, 19 листоп. 2020 р.). Харків : Право, 2020. С. 167-173.

8) Коновалова І. О. Щодо жертви електронного комерційного шахрайства. *Протидія злочинності і корупції : міжнародні стандарти та*

досвід України: зб. тез Міжнар. конф. (м. Харків, 22 вересня 2021 р.). Харків: Юрайт, 2021. С. 156-160.

9) Коновалова І. О. Загальносоціальні заходи запобігання електронному торгівельному шахрайству. *Наукові читання, присвячені пам'яті професора Т. А. Денисової : зб. матеріалів* (м. Запоріжжя, 10 березня 2022 р.). Запоріжжя : КПУ, 2022. С. 442-445.

List of publications of the applicant on the topic of the dissertation and information about the approbation of research results

Scientific works in which the main scientific results of the dissertation are published:

1) Konovalova I. O. Shakhraistvo i didzhytalizatsiia: istoryko-pravovyi analiz. *Pravo i suspilstvo*. 2021. Vyp. 3. S. 105-113.

2) Konovalova I. O. Zhertva v elektronnomu torhovelno-komertsiinomu shakhraistvi. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. Seriia : Pravo. Uzhhorod, 2021. № 65. S. 266-271.

3) Konovalova I. O. Dosvid zapobihannia shakhraistvu v sferi elektronnoi torhivli v SShA. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. Seriia : Pravo. Uzhhorod, 2021. № 68 (6). S. 220-225.

4) Konovalova I. O. Kryminolohichna kharakterystyka suchasnoho stanu shakhraistva u sferi elektronnoi torhivli. *Recht der Osteuropäischen Staaten*. 2022. № 1. S. 11-18.

Scientific works that certify the approbation of the dissertation materials:

5) Konovalova I. O. Do pytannia shakhraistv u sferi elektronnoi torhivli. *Protydiia orhanizovanii zlochynnosti i koruptsii : materialy KhIKh Vseukr. nauk. konf. z kryminolohii dlia studentiv, aspirantiv ta molodykh vchenykh* (m. Kharkiv, 2 hrud. 2019 r.). Kharkiv : Pravo, 2019. S. 69-71.

6) Konovalova Ilona. Modern forms of fraud. *Suchasne suspilstvo i nauka: aktualni doslidzhennia molodykh naukovtsiv : materialy Vseukrainskoi naukovo-*

praktychnoi Internet-konferentsii inozemnymy movamy., (Kharkiv, 29 travnia 2020 r.). Kharkiv : NIuU im. Yaroslava Mudroho, 2020. S. 56-58.

7) Konovalova I. O., Pyvovarov V. V. Shakhraistvo v umovakh didzhytalizatsii suspilstva. *Didzhytalizatsiia i bezpeka : materialy mizhnar. nauk.-prakt. konf.*, (Kharkiv, 19 lystop. 2020 r.). Kharkiv : Pravo, 2020. S. 167-173.

8) Konovalova I. O. Shchodo zhertvy elektronnoho komertsiinoho shakhraistva. *Protydiia zlochynnosti i koruptsii : mizhnarodni standarty ta dosvid Ukrainy: zbirnyk tez mizhnarodnoi konferentsii* (m. Kharkiv, 22 veresnia 2021 r.). Kharkiv: Yurait, 2021. S. 156-160.

9) Konovalova I. O. Zahalnosotsialni zakhody zapobihannia elektronnomu torhivelnomu shakhraistvu. *Naukovi chytannia, prysviacheni pamiati profesora T. A. Denysovoi : zbirnyk materialiv*. (m. Zaporizhzhia, 10 bereznia 2022 r.). Klasychnyi pryvatnyi universytet. Zaporizhzhia : KPU, 2022. S. 442-445.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ККУ – Кримінальний кодекс України.

SWIFT – Society for Wordwide Interbank Financial Telecommunication, Товариство всесвітніх міжбанківських фінансових телекомунікацій.

SEPA – Single Euro Payments Area, Єдина європейська мережа розрахунків.

SABRE – Semi-Automatic Business Research Environment, процедура резервування місць на авіарейси.

GTDI – General-purpose Trade Data Interchange, Стандарт обміну даними в міжнародних торгових організаціях.

EDIFACT – Electronic Data Interchange for Administration, Commerce and Transport, електронний обмін даними для управління, торгівлі та транспорту.

ВРУ – Верховна Рада України.

КМУ – Кабінет Міністрів України.

ЄС – Європейський Союз.

ІКТ – інформаційно-комунікаційні технології.

ООН – Організація Об'єднаних Націй.

США – Сполучені Штати Америки.

СОТ – Світова організація торгівлі.

EDI – електронний обмін даними.

КПК – Кримінальний процесуальний кодекс України.

ВВП – валовий внутрішній продукт.

ЮНКТАД – Конференція ООН з торгівлі та розвитку.

ОЕСР – Організація економічного співробітництва та розвитку.

CI – Consumer International, Міжнародна організація споживачів.

ECC Net – European Consumer Centres Network, Європейська мережа споживчих центрів.

FIAGC – Ibero-American Forum of Consumer Protection Agencies, Іберо-американський форум агентств із захисту прав споживачів.

CAN-SPAM – Controlling the Assault of Non-Solicited Pornography and Marketing Act, Закон про заборону спаму.

SAFE WEB – Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act, Закон здійснення боротьби зі спамом, шпигунським програмним забезпеченням і шахрайством.

FTC – Federal Trade Commission, Федеральна торговельна комісія.

FBI – Federal Bureau of Investigation, Федеральне бюро розслідувань.

HTTPS – Hypertext Transport Protocol Secure, безпечний протокол передачі гіпертексту.

НКРЗІ – Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації.

ЗМІ – засоби масової інформації.

РНБО – Рада національної безпеки і оборони України.

НКЦК – Національний координаційний центр кібербезпеки.

Мінекономіка – Міністерство економіки України.

Мінцифра – Міністерство цифрової трансформації.

ОМС – органи місцевого самоврядування.

Держспецзв’язок – Державна служба спеціального зв’язку та захисту інформації України.

CERT-UA – Computer Emergency Response Team of Ukraine, Команда реагування на комп'ютерні надзвичайні події України .

НБУ – Національний банк України.

ВСТУП

Обґрунтування вибору теми дослідження. Процес еволюціонування сучасної світової економіки тісно пов’язаний з розвитком інформаційного суспільства. Використання у комерційній діяльності й повсякденному житті найновіших комунікацій та технологій сприяло виникненню таких нових економічних понять, як «електронна комерція», «електронний бізнес» і «електронна торгівля».

Однак прискорення науково-технічного прогресу зумовлює не тільки динамічні позитивні зміни в розвитку електронному сегменті ринкових відносин, а й негативні тенденції розвитку у злочинному світі, призводить до появи нових кримінальних правопорушень. Так, в умовах суспільних трансформацій не лише залишилися традиційні види шахрайства, хоча й наповнені новітнім змістом, з використанням соціально-психологічних засобів впливу на свідомість, а й з’явилися принципово нові, вчинення яких стає можливим завдяки існуванню розгалуженої системи інформаційно-комунікаційних технологій, мобільного телефонного зв’язку, глобальної мережі Інтернет, електронних безготівкових розрахунків і переказів, банківських карток, інших різних інноваційних технологій тощо. Отже, крім шахрайства на звичному побутовому ґрунті, ці кримінальні правопорушення вже тісно пов’язані з бізнесом і вчинюються, зокрема, у сфері електронної торгівлі.

На сьогодні шахрайство у сфері електронної торгівлі поширюється в національному і глобальному кіберпросторі, тобто не має кордонів; пов’язане з цифровою трансформацією економіки, суспільства, держави й електронними комунікаціями між людьми (соціальними групами) у віртуальному середовищі, характеризується високою інтелектуальністю й високою латентністю. Більше того електронне комерційне шахрайство багатопрофільне, функціонує як організований злочинний бізнес.

Питання запобігання шахрайствам у сферах економіки й бізнесу, зокрема, у кредитно-фінансовій, банківській, медичній, туристичній сферах, на ринку корпоративних прав, нерухомості, страхування, торгівлі, висвітлювалися у роботах багатьох вітчизняних учених, а саме: П. П. Андрушка, А. М. Бабенка, О. М. Бандурки, В. Т. Білоуса, І. Г. Богатирьової, А. М. Бойка, В. В. Голіни, Б. М. Головкіна, В. К. Грищука, Н. О. Гуторової, І. М. Даньшина, О. Г. Колба, О. М. Костенка, Н. В. Кулакової, О. В. Лисодєда, О. М. Литвака, О. М. Литвинова, Ю. В. Луценка, М. І. Мельника, А. А. Музики, В. О. Навроцького, В. М. Поповича, О. В. Таволжанського, В. Я. Тація, В. П. Тихого, І. К. Туркевича, М. І. Хавронюка, В. В. Чернєя, А. Г. Чубенка, С. С. Яценка та ін.

Разом із тим, попри існування численних публікацій, питання вивчення кількісних і якісних показників шахрайства у сфері електронної торгівлі не було досліджено у працях науковців.

Аналіз повідомлень органів влади, громадських організацій, ЗМІ свідчить про зростання кількості таких випадків. Наприклад, загальний обсяг транскордонного шахрайства у США за 5 років виріс більш ніж у 2 рази, склавши у 2020 році 33 968 випадків, із заявленими збитками в розмірі 91,95 млн дол. США.

Усе вищезазначене свідчить про актуальність обраної теми, її нерозробленість у кримінології, наукову і практичну значущість й виступає відправною точкою для розв'язання проблем практики, визначення пріоритетів у науково-дослідній роботі, а також забезпечення спеціалізації підготовки фахівців відповідного профілю.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження узгоджується із Національною економічною стратегією на період до 2030 р. (затвердженою Постановою Кабінету Міністрів України від 3 березня 2021 року № 179), відповідає Стратегії розвитку наукових досліджень Національної академії правових наук

України на 2016 – 2020 рр. (затвердженої постановою загальних зборів Національної академії правових наук України від 3 березня 2016 р.). Робота виконана на кафедрі кримінально-правової політики Національного юридичного університету імені Ярослава Мудрого, в межах фундаментального дослідження «Теоретичні і прикладні проблеми запобігання злочинності та реформування державної кримінально-виконавчої служби в Україні» (номер державної реєстрації 0111U000958). Тема дисертації затверджена вченою радою Національного юридичного університету імені Ярослава Мудрого (протокол № 4 від 22 листопада 2019 р.).

Мета і завдання дослідження. Метою дисертації є надання кримінологічної характеристики шахрайству у сфері електронної торгівлі, визначення його детермінант, причин та умов вчинення кримінального правопорушення, розробка комплексу заходів запобігання досліджуваному явищу.

Досягнення поставленої мети обумовлює необхідність вирішення таких завдань:

1) на підставі аналізу теоретичних поглядів вчених визначити стан наукової розробленості проблеми;
2) розкрити організаційні та правові засади функціонування електронної торгівлі;
3) здійснити кримінологічний аналіз шахрайств у сфері електронної торгівлі;
4) встановити причини й умови вчинення шахрайств у сфері електронної торгівлі;
5) провести кримінологічний віктимологічний та психологічний аналіз взаємодії шахрая і жертви в електронному комерційному шахрайстві.
6) узагальнити міжнародний досвід запобігання шахрайствам у сфері електронної торгівлі;

7) сформулювати положення стосовно бачення системного підходу і шляхів загальносоціального запобігання шахрайствам у сфері електронної торгівлі;
8) визначити й схарактеризувати спеціально-кримінологічні заходи запобігання шахрайствам у сфері електронної торгівлі;
9) схарактеризувати суб'єктів запобігання шахрайствам у сфері електронної торгівлі.

Об'єктом дослідження є суспільні відносини, що виникають при вчиненні шахрайства у сфері електронної торгівлі.

Предметом дослідження є запобігання шахрайству у сфері електронної торгівлі.

Методи дослідження обрано відповідно до визначеної в роботі мети й завдань, з урахуванням об'єкта й предмета дослідження. При підготовці дисертації використовувалися такі методи: *діалектичний (філософський)* – для формулювання понять і визначень, тлумачення наукових термінів і приписів законодавства, інтерпретації статистичних даних (підрозділи 1.1, 1.2, 3.1, 3.2, 3.3); *системно-структурний* – для вивчення системи електронної торгівлі, кількісно-якісних показників шахрайств, які вчиняються у цій сфері, сукупності причин й умов протиправної поведінки, розроблення комплексу заходів запобігання й системи суб'єктів запобігання цим кримінальним правопорушенням (підрозділи 1.2, 2.1, 2.2, 3.2, 3.3); *статистичний* – для збирання, обробки й аналізу інформації за результатами емпіричного дослідження, узагальнення й аналізу даних електронних реєстрів і статистичних звітів (підрозділи 2.1, 2.3); *порівняльно-правовий* – для узагальнення міжнародного досвіду і кращих практик боротьби з шахрайством у сфері електронної торгівлі (підрозділ 3.1); *конкретно-соціологічні* – для надання кримінологічної характеристики досліджуваним злочинам, визначення рівня їх латентності, пізнання особливостей віктимної поведінки

жертв, надання рекомендації щодо напрямів і заходів запобігання цим злочинам (підрозділи 2.1, 2.3, 3.2).

Нормативно-правову базу дисертації складають: Конституція України, закони України, укази Президента України, постанови Кабінету Міністрів України, Кримінальний кодекс України, Кримінальний процесуальний кодекс України, відомчі нормативно-правові акти.

Емпіричну базу дослідження становлять: статистичні дані Генеральної прокуратури України щодо стану шахрайства і пов'язаних із ним кримінальних правопорушень за 2013 – 2021 рр.; узагальнені результати вибіркового вивчення 361 вироку, ухваленого судами України у 2011 р. та за період 2016 – 2021 рр., по кримінальних справах щодо шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки; результати експертного опитування 78 працівників Національної поліції України, прокуратури України, Служби безпеки України, судів та адвокатури України; результати анкетування громадян України, проведеного онлайн, з використанням Google-форм.

Наукова новизна отриманих результатів полягає в тому, що дисертація є першим в Україні кримінологічним дослідженням шахрайства у сфері електронної торгівлі як системного явища і різновиду економічної злочинності, що має власні тенденції розвитку, детермінуючий комплекс й особливості запобігання. За результатами дослідження сформульовано положення наукової новизни, що зводяться до такого.

Вперше:

– визначено поняття «шахрайство у сфері електронної торгівлі» з виокремленням головних його ознак, зумовлених об'єктивними закономірностями становлення електронної торгівлі в Україні, а саме: висока латентність; глобальний характер; вчинення кримінального правопорушення у кіберпросторі та віртуальному часі;

– розроблено комплексну кримінологічну і кримінально-правову характеристику шахрайств у сфері електронної торгівлі. Проаналізовано рівень, структуру й динаміку вказаних кримінальних правопорушень. Обґрунтовано положення про значну латентність цих злочинних діянь;

– встановлено, що жертва електронного комерційного шахрайства наділена специфічними характеристиками, які охоплюють не скільки соціально-демографічні, а переважно морально-психологічні групові риси. Констатовано, що взаємодія злочинця і жертви електронного комерційного шахрайства є дистанційною;

– запропоновано головні напрями й заходи спеціально-кримінологічного запобігання шахрайству у сфері електронної торгівлі, що включає: розробку і прийняття нормативно-правового акта про розвиток українського сегмента Інтернету; вдосконалення профільного законодавства у сфері електронної торгівлі; організацію повноцінної взаємодії правоохоронних органів, підприємств, установ, організацій всіх форм власності, ЗМІ з метою проведення інформаційно-виховної роботи серед населення щодо основних положень кібербезпеки; контроль й облік осіб, які схильні до вчинення вказаного типу кримінального правопорушення.

Удосконалено:

– положення щодо виокремлення способів вчинення шахрайств у сфері електронної торгівлі та залежно від цього даний вид злочину класифіковано на: шахрайство з авансовим платежем / повною або частковою передплатою, шахрайство з підміною товару, фішинг, шахрайство з вкраденими персональними банківськими даними, вішинг;

– перелік причин і умов шахрайства у сфері електронної торгівлі, до яких віднесено соціально-економічні, організаційно-управлінські та морально-психологічні групи;

– класифікацію суб’єктів запобігання шахрайству у сфері електронної торгівлі, запропоновано їх поділяти на: суб’єктів, які визначають державну

політику у сфері боротьби зі злочинністю (зокрема, запобігання кримінальним правопорушенням); суб'єктів, які координують діяльність із запобігання шахрайству у сфері електронної торгівлі; суб'єктів, які здійснюють правоохоронну діяльність у сфері боротьби з шахрайством у сфері електронної торгівлі; суб'єктів, діяльність яких напряму не пов'язана із запобіганням шахрайству у сфері електронної торгівлі, водночас безпосередньо впливає на усунення причин і умов відповідного кримінального правопорушення.

Набули подальшого розвитку:

– наукове обґрунтування необхідності вдосконалення положень законодавства про розвиток українського сегмента Інтернету, включення до спеціального закону положення про неприпустимість використання ІКТ у неправомірних цілях у сфері електронної торгівлі;

– доводи щодо нагальності оновлення профільного законодавства у сфері електронної торгівлі;

- наукові аргументи щодо потреби розроблення і запровадження спеціальних програм для боротьби з шахрайством;

– положення стосовно доцільності створення налагодженої взаємодії між існуючими суб'єктами запобігання електронному комерційному шахрайству.

Практичне значення отриманих результатів полягає в тому, що основні положення, висновки й рекомендації дисертаційного дослідження можуть бути використані: *у науково-дослідній сфері* – для подальших наукових розвідок за напрямом запобігання шахрайству у сфері електронної торгівлі; *у правотворчості* – для вдосконалення діяльності оперативних, превентивних і слідчих підрозділів Національної поліції України, зокрема Департаменту кіберполіції; *у правозастосовній сфері* – для удосконалення державної політики електронної торгівлі, законодавства у сфері кібербезпеки; *у навчальному процесі* – при підготовці навчально-методичних комплексів,

підручників, навчальних посібників з антикорупційних дисциплін і кримінології.

Особистий внесок здобувача. Викладені в дисертації положення, що становлять її новизну, є результатом самостійної роботи авторки. Наукові ідеї й розробки оприлюднені без співавторів у наукових фахових виданнях.

Апробація матеріалів дисертації. Основні наукові результати дисертації обговорювалися на всеукраїнських та міжнародних науково-практичних конференціях, а саме: XIX Всеукраїнській науковій конференції з кримінології для студентів, аспірантів та молодих вчених «Протидія організованій злочинності і корупції» (м. Харків, 2 грудня 2019 р.), Всеукраїнській науково-практичній інтернет-конференції іноземними мовами «Сучасне суспільство і наука: актуальні дослідження молодих науковців» (Харків, 29 травня 2020 р.), Міжнародній науково-практичній конференції «Діджиталізація і безпека»: (Харків, 19 листопада 2020 р.), Міжнародній конференції «Протидія злочинності і корупції» (м. Харків, 22 вересня 2021 р.), наукових читаннях, присвячених пам'яті професора Т. А. Денисової (м. Запоріжжя, 10 березня 2022 р.).

Структура та обсяг роботи. Дисертація складається з анотації, вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 220 сторінки, з них основний текст – 179 сторінок, список використаних джерел (236 найменування) – 27 сторінки.

РОЗДІЛ І
ПОНЯТТЯ ТА ОСОБЛИВОСТІ ШАХРАЙСТВА У СФЕРІ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

1.1 Генезис феномену шахрайства в умовах диджиталізації суспільства.

Розуміючи, що завданням даного підрозділу виступає аналіз генезису феномену шахрайства в умовах діджиталізації суспільства, беззаперечним є той факт, що таке шахрайство зумовлене розвитком класичного шахрайства, згадки про яке містяться в чималій кількості джерел права. Нижче розглянемо це більш детально.

Передусім наголосимо, що в семантичному значенні шахрайство – хитрий, спритний обман; крутійство; ошуканство; а шахрай – хитра, спритна й нечесна у своїх учинках особа. У схожому значенні загальновживаними категоріями є «аферист», «крутій», «махляр» (розм.), «жук» (розм.), «плутяга» (розм.), «комбінатор» (ірон., жарт.), «крутар» (діал.), «крючкодер» (заст.), «шарлатан» (неук, невіглас, який видає себе за фахівця) і «шулер» (картяр, який у грі користується нечесними прийомами) [1, с. 423; 3, с. 546].

Спираючись на те, що термін «генезис» означає процес походження, виникнення і становлення певного явища або процесу, вивчимо етапи, які, так би мовити, пройшло шахрайство.

Видається цілком логічним те, що підґрунтям для визначення певних періодів можуть стати історичні етапи формування, становлення й розвитку української державності. Ураховуючи це, можемо виокремити такі основні **фази генезису шахрайства**:

1) формування шахрайства за часів Київської Русі (X - XIII ст.);
2) становлення шахрайства, тобто від часів козацької доби – до періоду перебування України у складі Російської імперії (XIV ст. - 1917 р.);
3) розвиток шахрайства у радянський період (1917 - 1991 рр.);

4) сучасне шахрайство (з 1991 р. – по сьогодення).

Розглянемо кожен період окремо.

1. Формування шахрайства за часів Київської Русі (X-XIII ст.). Загальновідомо, що першою законодавчою пам'яткою Київської Русі (XI–XII ст.) була Руська Правда. Так, Правда у Короткій редакції (Коротка правда) містила статті щодо захисту майнових відносин, охорони приватної власності та встановлювала відповідальність за крадіжку (ст. 35–40). Однак статей щодо обману, зловживання довірою й шахрайства у документі не було. Перша згадка про зловживання довірою містилася у ст. 47 Просторової редакції Руської Правди, згідно з якою: «аже кто взищеть кун на друзе, а он ся начнеть запирати, то оже на нь выведеть послуси, то ти поидуть на роту, а он возьметь свое куны; зане же не дал ему кун за много лет, то плати ему за обиду 3 гривны». Одночасно, аналізуючи додаткову статтю Просторової редакції «О человеце»: «аже человек полгав куны у людей, а побежит в чюжю землю, веры ему не иняти, аки и татю»; відмічаємо, що в ній йдеться про діяння, пов'язане з обманом [2, с. 34]. Одним словом, згідно зі статтею особа, яка заволоділа чужими грошима в обманний спосіб, переховувалася на другій (чужій) землі.

2. Становлення шахрайства, від часів козацької доби – до періоду перебування України у складі Російської імперії (XIV ст. – 1917 р.). Починаючи з XIV ст. на території сучасної України почала активно розвиватися торгівля і, як наслідок, поширеними стали брехня й хитрість, які, вочевидь, сприяли розвитку шахрайства. У зв'язку з цим у Судебнику Івана Грозного 1550 року було встановлено наступне: «…а мошеннику та ж казнь, что и тату. А хто на оманщике взыщет и доведут на него, ино у ищеи иск пропал. А оманщика, как его ни приведут, ино его бити кнутьем» (ст. 58) [3, с. 148]. З цього приводу М. Ф. Владимирський-Буданов висловлює припущення, що дана норма уперше закріплює терміни «мошенник», «тать», «оманщик» і розмежовую шахрайство і крадіжки. Додамо, що, незважаючи на це, у

вищезгаданому документі перелік дій, які належать до шахрайських, залишився нерозритим.

Далі у Соборному Уложенні 1649 р. законодавець шахрайству присвятив окрему статтю: «О розбойных и о татиных делах» [4, с. 230–231]; а саме правопорушення прирівняв до татьби, учиненої вперше, хоча вид і міру покарання залишив такими саме.

У Військовому статуті Петра І, прийнятому в 1715 р., суворо каралися правопорушення проти власності (крадіжка, грабіж, пошкодження чужої речі), за їх вчинення встановлювалися покарання у виді спалювання, повішення, відрубування голови й каторги. Крім того, у документі містився перелік діянь, за способом вчинення близьких до шахрайства, таких як: фальшивомонетництво (арт. 199), обмір й обважування (арт. 200), виготовлення фальшивих печаток і документів (арт. 201); відповідальність за які не була вказана [5, с. 326; 363].

Історично важливою законодавчою пам'яткою XVIII ст. був Указ Катерини II «О суде и наказаниях за воровство разных родов и о заведении рабочих домов во всех Губерниях» 1781 року, розроблений для вирішення «настоящих различных недостатков, неясностей и неудобств, особливо же по делам уголовным», про що зазначалося в Преамбулі. Відповідно до Указу, «воровство» мало три різновиди: «воровство-грабеж», «воровство-кража» та «воровство-мошенничество». Так, про шахрайство йдеться в п. 5, згідно з яким «на торгу или в ином многолюдстве у кого из кармана что вынет, или обманом, или вымыслом, или внезапно у кого что отнимет, или унесет, или от платья полу отрежет, или позумент спорет, или шапку сорвет, или купя что не платя денег скроется, или обманом, или вымыслом продаст, или отдаст поддельное за настоящее, или весом обвесит, или мерой обмерит, или что подобное обманом или вымыслом себе присвоит ему не принадлежащее, без воли, или согласия того, чье оно» [6]. Таким чином, в Указі 1781 року вперше було визначено дії, які є шахрайськими: 1) кишенькова крадіжка; 2) раптове

викрадення чужого майна, розраховане на спритність та / або швидкість дій винного; 3) заволодіння чужим майном шляхом обману; водночас до обов'язкових ознак об'єктивної сторони шахрайства були віднесені місце, обстановка («на торгу или в ином многолюдстве», «внезапно») і спосіб вчинення кримінального правопорушення («обман или вымысел»).

За той час, коли життя українців поволі переходило до мирного стану й на передній план висувалися приватні інтереси людей, було здійснено кодифікацію «малоросійських законів», результатом якої стало прийняття «Прав, за якими судиться малоросійський народ» (1743 р.) – визначної пам'ятки українського права. Слід вказати, що у главі 24 «О ворахь и наказании и казни ихь, такожь и о протчем по деламь татейнымь» вищезазначеного Зводу законів містилися норми не тільки про крадіжку, а й про шахрайство, утім визначення даного поняття не наведено. Точніше, відповідно до п. 1 ар. 8 «Прав…», «воровь, мошенныковь, которые в день крадут разные вещи и явно похищал, за первымь пойманиемь на таком быть у столпа розгами или плетьми, за другимь, ухо резать, за третьимь нось урезати или на чель железамь знакь вижечь, а сверхь того наказания за другимь и за третьмь приводомь у столпа привязанныхь на публичномь месть быть розгами, либо плетми, а который бы ворь и по ономь трикратномь наказанеи быль паки на воровствь поймань, таковый имееть быть повешань» [7, с. 429 - 430]. Відзначимо, що у «Правах…» законодавець виокремив кваліфіковані види шахрайств залежно від повторюваності вчиненого кримінального правопорушення.

Згодом, а саме у 1832 році, прийнято Звід законів Російської імперії, за яким шахрайство розглядалося в такому ж значенні, що й раніше. Проте в акті наведено більш детальну його кваліфікацію залежно від розміру завданої шкоди (до 5 руб.; від 5 руб. до 10 руб.; від 10 руб. до 15 руб.; від 15 руб. до 20 руб.; від 20 руб. до 100 руб.; понад 100 руб.) та встановлено відповідальність за «подлоги в имуществах и лживых поступках».

Пізніше в Уложенні про покарання кримінальні та виправні 1845 року шахрайство трактується через більш сувору юридичну конструкцію, а саме: «воровством-мошенничеством признает всякое, посредствам какого-либо обмана учиненное, похищение чужих вещей, денег или иного движимого имущества; мера наказания за которое, определяется по степени большой или меньшей предумышленности преступления, по свойству употребленных для совершения его средств и по другим обстоятельствам, больше или меньше увеличивающие или уменьшающие вину преступника» (ст. 2172). Таким чином, законодавець уперше у даному формулюванні до предмета шахрайства відніс речі, гроші та інше рухоме майно і визнав за даним видом кримінального правопорушення інтелектуальний спосіб заволодіння чужим майном. Нагадаємо, що раніше шахрайство розглядалося як діяння, учинене за допомогою спритності й хитрощів винного. Крім того, в Уложенні були визначені обставини, які обтяжують покаранням: 1) вчинене «по предварительному соглашению и уговору нескольких лиц и было последствием обдуманного заранее намерения или умысла; 2) когда для обмана были виновным приготовлены особые какие-либо орудия или вещи, или же сделаны иные нарочно для того приготовления; 3) когда виновный по званию своему или месту, или же по особым к лицу им обманутому отношениям, долженствовал внушать и особую к себе доверенность; 4) когда он обманул таким образом малолетнего, или же слепого или глухонемого; 5) когда преступление, учинено во второй раз (ст. 2181)» [8].

Згодом, а саме у 1903 р., Миколою II затверджене Кримінальне уложення – останній кодифікований кримінально-правовий акт Російської імперії, робота над яким тривала 22 роки. До його прийняття суспільні відносини між державою й особами, які вчинили кримінальні правопорушення (кримінально-правові суспільні відносини), регулювалися Уложеннями про покарання кримінальні та виправні 1857 р., 1866 р., 1885 р., останні документи жодних змін у визначенні поняття шахрайства та відповідальності за його вчинення не містили. Аналогічно

у Кримінальному уложенні 1903 р. шахрайству присвячено окрему главу, а саме 33 «О мошенничестве». Відповідно до ст. 591 згаданого Уложення шахрайство визначалося як: «1) похищение, посредством обмана, чужого движимого имущества, с целью присвоения; 2) похищение чужого движимого имущества, с целью присвоения, посредством обмера, обвеса или иного обмана в количестве или качестве предметов при купле-продажи или иной сделке; 3) побуждение, посредством обмана, с целью доставить себе или другому имущественную выгоду, в уступке права по имуществу или ко вступлению в иную невыгодную сделку по имуществу» [9]. Важливо те, що згідно зі статтею предметом кримінального правопорушення могло бути не лише рухоме, а й нерухоме майно.

3. Розвиток шахрайства у радянський період (1917 – 1991 рр.). Наступний етап генезису кримінального законодавства, у тому числі й шахрайства, розпочався у 1917 р. і характеризувався тим, що в радянський період закон про кримінальну відповідальність «обслуговував» ті важливі соціально-політичні, економічні й правові завдання, що вирішувала держава на певній стадії свого розвитку. Сказане підтверджується нормами Декрету ВЦВК «Про відміну приватної власності на нерухомість у містах» 1917 року, за яким «отменяется право частной собственности на все без исключения участки, как застроенные, так и не застроенные, как принадлежащие частным лицам и промышленным предприятиям, так и ведомствам и учреждениям, находящиеся в пределах всех городских поселений» [10]. Як наслідок, робота правоохоронних і судових органів переважно була зосереджена на боротьбі з крадіжками, грабежами, спекуляцією й бандитизмом. У своїй діяльності вони керувалися Уложенням 1885 року і кримінальним Уложенням 1903 р. у тих частинах, які не суперечили нормам Декретів РНК РСФРР «О суде» № 1 та «О суде» № 2, відповідно до яких «местные суды решают дела именем Российской Республики и руководятся в своих решениях и приговорах законами свергнутых правительств лишь постольку, поскольку таковые не

отменены революцией и не противоречат революционной совести и революционному правосознанию» [11, с. 124].

Перший радянський кримінальний кодекс (далі – КК) був прийнятий 1 червня 1922 року. У ньому законодавець визначив шахрайство як «получение с корыстной целью имущества или права на имущество посредством злоупотребления доверием или обмана» (ст. 187). З одного боку, у примітці до зазначеної статті законотворець розкрив суть поняття «обман» як «сообщение ложных сведений, так и заведомое сокрытие обстоятельств, сообщение которых было обязательно» [12]; проте з другого – не надав визначення категорії «зловживання довірою».

Після цього відповідно до КК РСФРР, прийнятого в 1926 р., шахрайство розглядалося як «злоупотребление доверием или обман в целях получения имущества или права на имущество или иных личных выгод» (ст. 169) [13], тобто кримінальне правопорушення вважалося закінченим на ранній стадії – із моменту вчинення обману або зловживання довірою (усічений склад злочину); на відміну від норм КК РСФРР 1922 року, де воно визнавалося таким із моменту заволодіння винним майном або придбанням права на нього. У підрозділі ІІІ «Визначення міри покарання» КК УСРР 1922 року передбачалось, що «при визначенні міри покарання враховується ступінь і характер небезпеки як самого злочинця, так і вчиненого ним злочину». Для встановлення цього «вивчається обстановка вчинення злочину, з'ясовується особа злочинця», а також «встановлюється, наскільки сам злочин у даних умовах часу і місця порушує засади суспільної безпеки» (ст. 24). З урахуванням цього «для визначення міри покарання» передбачалося враховувати: 1) «чи вчинений злочин в інтересах відновлення влади буржуазії, або в інтересах виключно особисто того, хто вчинив злочин»; 2) «чи спрямований злочин проти держави або окремої особи»; 3) «чи вчинений злочин у стані голоду і потреби або ні»; 4) «чи вчинений злочин з принизливих, корисливих спонукань або без них»; 5) «чи вчинений злочин з повним

усвідомленням заподіяної шкоди або із зневаги та несвідомості»; 6) «чи вчинений злочин професійним злочинцем чи рецидивістом, або він вчинений у перший раз»; 7) «чи вчинений злочин групою (шайкою, бандою) або однією особою»; 8) «чи вчинений злочин шляхом насильства або без нього»; 9) «чи виявлений особою, яка вчиняє злочин, заздалегідь обдуманий намір, жорстокість, хитрість, або злочин вчинений у стані запалу, з необережності, легковажності, або під впливом погрози і примусу з боку іншої особи» (ст. 25). [14, с. 277].

У цей період держава приділяла значну роль захисту державної соціалістичної власності від різного роду корисливих посягань. З огляду на це у КК РСФРР 1926 р. за «мошенничество, имевшее своим последствием причинение убытка государственному или общественному учреждению» (ч. 2 ст. 169) було встановлено більш сувору відповідальність, а саме у вигляді позбавлення волі на строк до 5 років із конфіскацією всього або частини майна, ніж за шахрайство, яке завдавало шкоди приватній власності громадян (позбавлення волі до 2 років). Крім того, до кваліфікованих видів шахрайств віднесено: «подделка в корыстных целях официальных бумаг, документов и расписок» (ст. 170) та «обманное изменение с корыстной целью вида или свойства предметов, предназначенных для сбыта или общественного употребления, если это имело или могло иметь последствием причинение вреда здоровью, а равно сбыт таких предметов» (ст. 171).

Характерно, що радянська влада особливу увагу приділяла зміцненню соціалістичної (державної, колгоспної та кооперативної) власності, підтвердженням цього є Закон «Об охране имущества государственных предприятий, колхозов и кооперации и укреплении общественной (социалистической) собственности», прийнятий ЦВК та РНК 7 серпня 1932 р. [15]. На думку істориків, даний нормативно-правовий акт є репресивним, оскільки згідно з його нормами відповідальність за «хищение» майна каралася найбільш сурово, у виді смертної кари.

У післявоєнний період кримінальне законодавство характеризувалося відсутністю єдиних норм щодо «хищения» соціалістичної та особистої власності громадян, відповідна група відносин регулювалася указами ВР СРСР «Об уголовной ответственности за хищение государственного и общественного имущества» й «Об усилении охраны личной собственности граждан» 1947 р.

У КК РРФСР 1961 р. норми, які встановлювали відповідальність за шахрайство щодо соціалістичної та приватної власності, розміщувалися в різних главах. Так, відповідно до ст. 93 глави II «Преступления против социалистической собственности» шахрайство визначалося як «завладение государственным или общественным имуществом путем обмана или злоупотребления доверием» [16], а обтяжуючими обставинами: 1) шахрайство, вчинене повторно або за попередньою змовою групою осіб; 2) шахрайство, що завдавало суттєвих збитків державі або громадській організації чи вчинене особливо небезпечним рецидивістом. Водночас, у ст. 147 глави V «Преступления против личной собственности граждан», шахрайство трактувалося як «завладение личным имуществом граждан или приобретение права на имущество путем обмана или злоупотребления доверием». Зі сказаного раніше випливає, що за КК 1961 р. предметом шахрайства проти соціалістичної власності було рухоме й нерухоме майно, тоді як проти особистої власності громадян – не лише майно, а й право на нього.

4. Сучасне шахрайство (з 1991 р. – по сьогодення). Після проголошення незалежності Верховна Рада України (далі – ВРУ) прийняла новий Кримінальний кодекс України (далі КК України), який набув чинності 5 квітня 2001 р. Так, стаття 190 даного акту визначає шахрайство як заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою [17]. Згодом у постанові Пленуму Верховного суду України від 6 листопада 2009 р. № 10 «Про судову практику у справах про злочини проти власності» було здійснено роз’яснення даної норми, а саме

уточнено, що обман чи зловживання довірою при шахрайстві застосовуються винною особою з метою викликати у потерпілого впевненість у вигідності чи обов'язковості передачі їй майна або права на нього. Крім того, роз'яснено, що обман – це повідомлення потерпілому неправдивих відомостей або приховування певних обставин, а зловживання довірою – це недобросовісне використання довіри потерпілого. Все уже сказане означає те, що обов'язковою ознакою шахрайства є добровільна передача потерпілим майна чи права на нього [18]. Іншими словами, шахрайство полягає у протиправному заволодінні чужим майном або придбанні права на майно шляхом обману потерпілого чи зловживання довірою. У згаданій постанові Пленуму наголошено, що особа, у віданні або під охороною якої знаходиться майно, сама передає таке майно винному, вважаючи, що останній має право на нього. Особливістю шахрайства є те, що шахрай викликає в потерпілого бажання передати йому майно чи уступити право на майно. З огляду на це введений в оману потерпілий добровільно передає винному майно чи право на нього [19, с. 165 - 166].

Зауважимо, що кваліфікованими й особливо кваліфікованими видами даного кримінального правопорушення є шахрайство: 1) вчинене повторно або 2) за попередньою змовою групою осіб (ч. 2 ст. 190), або 3) у великих розмірах, або 4) шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190), або 5) в особливо великих розмірах, або 6) організованою групою (ч. 4 ст. 190); 7) що заподіяло значної шкоди потерпілому (ч. 2 ст. 190).

Таким чином, у КК України закріплено два способи вчинення шахрайства: обман і зловживання довірою. Перший спосіб полягає в повідомленні неправдивих відомостей, які являють собою перекручену інформацію про певні обставини, події, явища, що не відповідають дійсному стану справ і викривлюють істину; а також у неповідомленні (або замовчуванні) тих відомостей, які винний повинен був повідомити. Так, на

думку М. І. Панова, обман буває двох видів: 1) той, що вчиняється шляхом дії (активна форма поведінки особи, яка говорить неправду), тобто повідомлення неправдивих відомостей; та 2) обман, вчинений шляхом бездіяльності (пасивна форма поведінки), йдеться про замовчування, неповідомлення тих відомостей, які суб'єкт повинен був повідомити [20]. Другий спосіб – зловживання довірою, що означає недобросовісне використання довіри з боку власника або іншої особи, у віданні якої знаходиться майно. Частіше за все підґрунтям зловживання довірою є особисте знайомство, родинні, дружні зв'язки, рекомендації інших осіб, цивільно-правові або трудові відносини [19, с. 166 - 167].

Далі (умовно кажучи, у другій частині даного підрозділу) розглянемо феномен шахрайства в умовах діджиталізації суспільства, а для досягнення поставленої мети охарактеризуємо взаємозв'язок шахрайства з глобальними суспільно-економічними процесами.

Перш за все відмітимо, що світова економіка переживає період незворотних трансформацій. Загальновизнано, що XXI століття знаменується активним формуванням шостого технологічного укладу й ризиками, з якими стикається цивілізація внаслідок упровадження новітніх технологій. Сьогодні відбуваються драматичні зміни не лише в геополітичній площині, а у й сфері розподілу центрів впливу на найважливіші об'єкти інфраструктури безвідносно до їх територіальної або інституціональної належності з одночасним формуванням стратегічних центрів управління ними в інтересах суб'єктів управління, у тому числі транснаціональних корпорацій [21, с. 218].

Водночас розвинені країни стоять на порозі четвертої промислової революції. У контексті наведеного зауважимо, що термін «революція» означає докорінний переворот у певній сфері суспільного життя або різкий стрибкоподібний перехід від одного якісного стану до іншого. Відмінними рисами революції є різкість і швидкість змін глобального характеру.

Варто нагадати, що починаючи з другої половини XVIII ст. у світі відбулися чотири промислові революції. Так, результатом першої була індустріалізація країн Європи; другої – розвиток засобів комунікацій та економіки; третьої – комп'ютеризація виробництва. Сьогодні суспільство проживаємо четверту промислову революцію або, як її ще називають, Індустрію 4.0[1], яка, на думку засновника теорії постіндустріального суспільства Деніела Белла, розгортається у сфері телекомунікацій.

Примітно, що наприкінці XIX – у першій половині XX ст. основними засобами комунікації були газети, журнали, книги, телеграфи, телефони, радіо й телебачення, тоді як уже у другій половині XX ст. дану нішу зайняв комп'ютерний зв'язок, витіснивши вказані засоби. На переконання Д. Белла, можна виокремити такі головні завдання Індустрії 4.0: 1) злиття телефонної й комп'ютерної систем, телекомунікацій та обробки інформації в одну модель; 2) заміна паперу електронними засобами; 3) розширення телевізійної служби через кабельні системи; 4) реорганізація системи зберігання інформації та системи запиту інформації на базі комп'ютерів в інтерактивну інформаційну мережу, доступну всім; 5) розширення системи освіти на базі комп'ютерного навчання [22, с. 141]. На додачу до всього вищезгаданого зазначимо, що найбільшим досягненням четвертої промислової революції стала тотальна цифровізація підприємств (тобто використання безпілотних транспортних засобів, 3D-друку, передової робототехніки, нанотехнологій, біотехнологій, штучного інтелекту та ін.), завдяки чому значна кількість товарів і послуг стала значно дешевшою, наприклад, електронні книжки коштують у два рази менше за паперові. Крім того, засновник Всесвітнього економічного форуму (WEF) Клаус Шваб описує промислову революцію 4.0 так: вона стирає межі між фізичними, цифровими й біологічними сферами [23, с. 36].

[1] Термін Індустрія 4.0 запропоновано для позначення четвертої промислової революції у 2011 році на Ганноверському ярмарку, а у 2013 році в Німеччині, в опублікованому збірнику документів під заголовком «Smart Manufacturing for the Future» *(MacDougall, 2014),* «введенно» поняття «Industry 4.0».

Головним «продуктом» четвертої промислової революції стала цифрова економіка, яку вчені в цілому характеризують як динамічну економіку, що базується на активному впровадженні інновацій та інформаційно-комунікаційних технологій в економічну діяльність та інші сфери життєдіяльності суспільства. Це дозволяє підвищити ефективність і конкурентоспроможність окремих компаній, економік, а також покращити рівень життя населення [24, с. 14]. Звернемо увагу на визначення Департаменту комунікацій та цифрової економіки Австралії, відповідно до якого цифрова економіка – це глобальна мережа економічних і соціальних заходів, реалізованих через такі платформи, як Інтернет, мобільні й сенсорні мережі [25, с. 10].

Цифрова економіка, як стверджував Томас Мезенбург, складається з 3-х компонентів:

1) інфраструктури електронного бізнесу, яка сприяє його ефективній роботі (апаратне і програмне забезпечення, телекомунікації, мережі тощо);
2) електронного бізнесу, який провадять через комп'ютерно-опосередковані мережі.
3) електронної комерції – продажу товарів і послуг (або дистрибуції товарів) через Інтернет.

Слід підкреслити, що відповідно до прийнятої Кабінетом Міністрів України (далі – КМУ) у січні 2018 р. Концепції розвитку цифрової економіки та суспільства на 2018 – 2020 роки, цифрова економіка – це діяльність, у якій основними засобами (факторами) виробництва є цифрові (електронні, віртуальні) дані як числові, так і текстові. Іншими словами, цифрова економіка базується на інформаційно-комунікаційних і цифрових технологіях, стрімкий розвиток і поширення яких впливають на традиційну (фізично-аналогову) економіку, трансформуючи її від такої, що споживає ресурси, до економіки, що їх створює [26].

Нині цифрова економіка стрімко розвивається в глобальних масштабах, перетворюючись на двигун інновацій, підвищення конкурентоспроможності, економічного зростання. Останнім часом прослідковується тенденція, відповідно до якої розвинені країни перенаправляють свою діяльність у цифрові економічні моделі. Відбувається глобальний перехід до digital або ж, одним словом, діджиталізація суспільства.

Термін «діджиталізація» походить від англійського «digitalization» і в перекладі означає «оцифрування», «цифровізація», «приведення в цифрову форму». Поряд із вищезазначеними поняттями у схожому значенні вживаються категорії «діджитизація», «дігіталізація», «цифрова трансформація».

Як відмічає Ж.-П. де Клерк, діджиталізація – це процес використання цифрових технологій і даних (оцифрованих/діджиталізованих та існуючих у цифровій формі спочатку) із метою отримання прибутку, поліпшення бізнесу, зміни/трансформації бізнес-процесів і створення належного середовища для їх реалізації, в основі якого лежить використання цифрової інформації [27, с. 181].

Зазначимо, що у Плані дій «Підприємництво 2020» («Entrepreneurship 2020 Action Plan») Європейського Союзу (далі – ЄС) передбачено проведення політики цифровізації підприємництва у п’яти вимірах: 1) бази цифрових знань і ринку інформаційно-телекомунікаційних технологій; 2) цифрового бізнес-середовища; 3) доступу до фінансів; 4) цифрових навичок і електронного лідерства; 5) підприємницької культури.

Першочерговим на шляху до діджиталізації був розвиток інформаційно-комунікаційних технологій (далі – ІКТ), тобто різноманітних технологічних інструментів і ресурсів, які використовуються для забезпечення процесу комунікації, створення, поширення, збереження й управління інформацією [28, с. 7]. Пізніше ІКТ разом із глобальною мережею Інтернет стали рушійною силою нової економіки. Важливо те, що у 2021 році кількість користувачів

Інтернету у світі зросла з 4,1 до 4,9 мільярда, у порівнянні з 2019, зокрема, через пандемію COVID-19. Найвищий відсоток користувачів світової павутини прослідковано в Європі, а найнижчий – в Африці [29]. Водночас кількість українських інтернет-користувачів у 2021 році також зросла на 2 млн, що на 33 % більше, ніж у 2019 році, і на початку 2021-го становила майже 30 млн, тобто приблизно 67 % населення країни [30]. Зауважимо, що ВВП країн, як видається, дуже залежить (пов'язаний) від проникнення Інтернету, при цьому найбагатші країни мають вищу пропускну здатність Інтернету й навпаки. Різниця між користувачами Інтернету в Північній Кореї та Катарі становить 98,4 % [31].

Завдяки бурхливому розвитку інноваційних технологій відбувся процес діджиталізації банківського сектору[2]. Спочатку, а саме у 80-х роках XX ст., західні банки почали надавати деякі послуги в режимі онлайн. У такий спосіб клієнт міг зайти на сайт банку й виконати певні операції, використовуючи при цьому надані йому паролі. До речі, електронний банкінг являє собою технологію віддаленого банківського обслуговування – «home banking» («віддалений» або «домашній» банкінг). За допомогою цієї послуги можна отримати банківську інформацію загального користування, зокрема, щодо умов вкладів, видання позик, курсів валют; здійснити купівлю-продаж валюти; відкрити депозит; отримати авторизовану інформацію про стан рахунків (залишки, обороти, виконання виписок за певний період); здійснити оплату товарів, страхових полісів, комунальних послуг; поповнити карткові рахунки онлайн. Щороку кількість тих, хто послуговується електронним банкінгом, зростає в арифметичній прогресії. Цікаво, що за версією FinAward 2021 року перше місце в номінації «Найкращий мобільний додаток» отримав «monobank | Universal Bank», у той час, як у номінації «Провідні технології та інновації (банки)» – «Приватбанк» [32].

[2] створення банкоматів, банківських терміналів, електронного-банкінгу, та більше того - оплати товарів та послуг безконтактно, за допомогою технологій Pay Pass або дотиком телефону.

Підкреслимо, що починаючи з другої половини XX століття діджиталізація банківського сектору відбувається на глобальному рівні. У 1973 році у Брюсселі (Бельгія) створено Товариство міжнародних міжбанківських фінансових телекомунікацій (Society for Wordwide Interbank Financial Telecommunication, SWIFT) – міжнародну міжбанківську систему передавання інформації та здійснення платежів, послугами якої користуються близько 11 тисяч банків і фінансових установ з понад 210 країн. До того ж у лютому 2014 року на території Європейського Союзу засновано єдину зону SEPA (англ. Single Euro Payments Area), яка встановила єдиний європейський порядок безготівкових платіжних операцій в межах Європейської економічної зони (27 країн – членів Європейського Союзу, а також Норвегії, Ісландії, Ліхтенштейну та Швейцарії) у валюті євро.

Слід враховувати, що з появою електронних і віртуальних грошей у людей кардинально змінилося уявлення і ставлення до традиційних грошей. Додаймо, що електронні гроші – це одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу іншими, ніж емітент, особами і є грошовим зобов'язанням емітента [33]. Також новацією останніх років стали віртуальні гроші (або криптовалюта) – цифрова валюта, яка функціонує завдяки механізму асиметричного цифрування. У світі налічується понад тисячу цифрових валют, найвідомішою з них є bitcoin (біткойн). Зауважимо, що 17 лютого 2022 р. ВРУ повторно ухвалила у другому читанні Закон «Про віртуальні активи», яким передбачено комплексне врегулювання правовідносин, що виникають у зв'язку з обігом віртуальних активів в Україні, визначено права й обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обігу віртуальних активів. Згідно зі згаданим Законом віртуальний актив – це нематеріальне благо, що є об'єктом цивільних прав, має вартість і виражене сукупністю даних в електронній формі. Існування й оборотоздатність віртуального активу стають можливими завдяки системі забезпечення його обороту. До речі, віртуальний актив може

посвідчувати майнові права, зокрема, права вимоги на інші об’єкти цивільних прав [34].

На додачу до всього вищезгаданого зауважимо, що серед науковців існує гіпотеза, відповідно до якої у світових валютно-фінансових і кредитних відносинах віртуальна валюта може призвести до глобальних змін, оскільки заперечує доларовий стандарт. Як відомо, світова економіка базується на доларі США – домінуючій світовій резервній валюті. Однак така ситуація не може тривати вічно через те, що суперечить інтересам інших держав. З огляду на це вчені припускають, що влада нових індустріальних держав боротиметься за включення своїх національних грошових одиниць до списку домінуючих світових валют або використовуватимуть альтернативну глобальну валюту. Саме в цьому випадку можливий перехід від Ямайської валютної системи до міжнародної системи криптовалют, а такі світові валюти, як долар США та євро, можуть втратити свої преференції.

На нашу думку, дана позиція є спірною. У свою чергу, відмічаємо, що послугування електронними й віртуальними грошима приводить до нівелювання необхідності обороту паперових грошей, через що трансформується значення економічної категорії «гроші» (як матерії). Раніше оборот грошей здійснювався через особистий контакт двох або більше осіб, в основу якого покладалися довірливі відносини, утім сьогодні це стає «пережитком СРСР». Тому в контексті життєвої відмінності «класичного» від сучасного електронного шахрайства варто розуміти наступне: якщо грошей мало і вони матеріальні, то ними доволі важко заволодіти. Однак зовсім інші реалії, як показує вищенаведений аналіз, пропонує сучасним шахраям діджиталізована економіка.

Так само інтернаціоналізація господарської діяльності наприкінці XX ст. вступила в стадію економічної глобалізації, відбулися численні зміни в економіці, пов’язані передусім зі створенням транснаціональних корпорацій. У цілому під економічною глобалізацією варто розуміти об’єктивні процеси

зростання економічної взаємодії держав через активну інтеграцію національних ринків товарів, послуг і капіталів. Як наслідок, світовий простір поступово перетворюється на єдину зону з вільним рухом товарів, послуг і капіталу, можливостями вільно поширювати ідеї, стимулюючи розвиток державних інститутів і вдосконалюючи механізми їх взаємодії. Зрештою, глобалізація економіки зумовлює: 1) транснаціоналізацію торгівлі товарами, послугами, технологіями, об'єктами інтелектуальної власності; 2) міжнародний рух інфраструктури виробництва (робочої сили, капіталу, інформації); 3) модернізацію міжнародних фінансово-кредитних і валютних операцій; 4) налагодження виробничої, науково-технічної, технологічної, інженерної й інформаційної співпраці. Таким чином, глобалізація формує міжнародно-правовий і культурно-інформаційний простір як інфраструктуру обміну товарами, послугами, капіталами тощо.

Підсумовуючи, наголосимо, що всі вищеперераховані суспільно-економічні процеси прямо або опосередковано впливають на злочинність. Краще сказати, що зростає питома вага кіберзлочинності, ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Підвищується технічний рівень реалізації кіберзлочинності, постійно вдосконалюються й розробляються нові інструменти й механізми кіберзлочинів [35], що провокує еволюціонування шахрайства у сфері електронної торгівлі.

По-перше, злочинність набуває професійних й інтелектуальних ознак. Особи, які багаторазово вчиняли злочини, досягають певної майстерності (професіоналізму) і не бажають відмовлятися від такої поведінки, розраховуючи на безкарність. Стосовно цього В. В. Голіна зауважує, що більш виразно професійна злочинність проявляється у корисливих злочинах, адже це пояснюється жадібним ставленням злочинця до «легких грошей» [36, с. 246–247].

По-друге, як вже було зазначено, злочинність набуває нових організованих форм. У Концепції державної політики у сфері боротьби з організованою злочинністю, схваленій розпорядженням КМУ від 16 вересня 2020 р. № 1126-р, відмічається, що відсутність системного підходу до ведення боротьби з організованою злочинністю, неналежний рівень взаємодії правоохоронних органів у відповідній сфері, застаріле й розбалансоване нормативно-правове забезпечення з питань боротьби з організованою злочинністю, недосконаліть процедури моніторингу криміногенної ситуації, відсутність консолідованої об'єктивної методології оцінки загроз організованої злочинності, використання застарілих форм і методів боротьби з таким явищем призводить до загострення проблем, пов'язаних з організованою злочинністю, і низького рівня ефективності боротьби з нею [37]. Згідно з Законом України від 30 червня 1993 року № 3341-XII «Про організаційно-правові основи боротьби з організованою злочинністю», організована злочинність – це сукупність злочинів, що вчиняються у зв'язку зі створенням і діяльністю організованих злочинних угруповань [38]. Характерно, що вона досить динамічна, оскільки швидко реагує на зовнішні фактори. Основними ознаками організованих злочинних угруповань є достатньо високий рівень організованості та стійкі корупційні й міжнародні злочинні зв'язки. Звертаємо увагу на визначення організованої економічної злочинності вченого І. В. Маслія як нелегального, тобто такого, що знаходиться поза законом, соціального інституту, який відкрито змагається з легальними державними інститутами й виступає загальносуспільною небезпекою для економіки країни. Також, на його думку, фінансово-економічній організованій злочинності притаманні такі основні характеристики: 1) широке використання комп'ютерної техніки, засобів мережі Інтернет для ведення організованої злочинної діяльності; 2) проведення організованої злочинної діяльності під «прикриттям» легальних підприємницьких, банківських структур; 3) використання схем навмисного

доведення до банкрутства з подальшим викупом; 4) прагнення отримати контроль над найбільш прибутковими сферами економіки; 5) широке використання недоліків у чинному законодавстві задля розробки й застосування зі злочинною метою схем, особливо у бюджетній сфері [39, с. 95–96].

По-третє, відбувається процес корпоратизації злочинності, індивідуальна злочинність поступається місцевій груповій, групова переростає в організовану, а остання, виходячи на міжнародний рівень, стає корпоративною [40, с. 310]. Безумовно, такий процес пов'язаний з транснаціональною або транскордонною злочинністю. Повне визначення поняття «транснаціональна злочинність» міститься в документах Всесвітньої конференції в Неаполі (1994 р.), виходячи з приписів яких вона розглядається як здійснення злочинними організаціями незаконних операцій, пов'язаних із переміщенням потоків інформації, грошей, фізичних об'єктів, людей, інших матеріальних і нематеріальних засобів через державні кордони з метою використання сприятливої ринкової кон'юнктури в одній або кількох іноземних державах та/або отримання суттєвої економічної вигоди, а також ефективного ухилення від соціального контролю за допомогою корупції, насильства та урахування значних відмінностей у системах кримінального правосуддя різних країн [41, с. 220].

Отже, технічний прорив і глобалізація економіки синергетично вплинули на суспільство. У даних умовах шахрайство не зникає, воно змінюється. Серед факторів, які позначилися на цьому процесі, виокремлюємо: 1) четверту промислову революцію; 2) цифрову економіку; 3) глобалізацію світового співробітництва й економіки; 4) діджиталізацію суспільства; 5) стрімкий розвиток ІКТ і мережі Інтернет; 6) діджиталізацію банківського сектору; 7) зміну традиційних функцій грошей; 8) професіоналізацію й інтелектуалізацію злочинності; 9) трансформацію індивідуальної злочинності в організовані форми; 10) корпоратизацію злочинності; 11) корупцію.

Таким чином, світ змінився – став віртуальний. Разом із цим трансформується шахрайство, воно набуває нових, раніше невідомих форм. У попередньому значенні поняття «шахрайство» зосереджувалися на особистому контакті шахрая і жертви, зараз же – на способі посягань. Незмінним залишається корисливий мотив – бажання отримати те, що не належить шахраю.

Крім того, сучасному шахрайству притаманні наступні кримінологічно-значущі риси: 1) великий рівень суспільної небезпеки; 2) інтелектуальність; 3) висока латентність; 4) вчинення кримінального правопорушення у кіберпросторі й віртуальному часі; 5) суттєве віктимологічне й психологічне наповнення «віддаленої» моделі взаємодії шахрая і жертви (групової жертви).

Звертаємо увагу на те, що кримінологічними дослідженнями шахрайства за часів незалежності нашої держави займалися: А. М. Бабенко [42; 43; 44] (крадіжка і шахрайство як види корисливих кримінальних правопорушень проти власності: соціально-правова та віктимологічна характеристика, 2023 р.), О. В. Лисодєд (кримінологічні проблеми шахрайства, 1999 р.) [45], П. М. Коваленко (запобігання шахрайству на фінансових ринках у біржовій торгівлі, 2005 р.) [46], А. В. Микитчик (кримінологічні засади запобігання шахрайству з нерухомістю, 2008 р.) [47], В. Л. Пластун (проблеми страхового шахрайства та практика його уникнення, 2009 р.) [48], І. А. Нестерова (злочинність у сфері туристичного бізнесу: кримінологічна характеристика та запобігання, 2016 р.) [49], а також науковці із суміжних дисциплін кримінального права та криміналістики: О. Л. Мусієнко (теоретичні засади розслідування шахрайства в сучасних умовах, 2007 р.) [50], Ю. В. Луценко [51; 52] (кібербезпека та інформаційна безпека, 2022 р.), Н. В. Павлова (особливості розслідування шахрайства, пов’язаного з відчуженням приватного житла, 2007 р.) [53], І. В. Іщук (початковий етап розслідування шахрайств у сфері страхування автотранспортних засобів, 2010 р.) [54], С. С. Чернявський (теоретичні та практичні основи методики розслідування фінансового шахрайства, фінансове

шахрайство: методологічні засади розслідування 2010 р.) [55], О. В. Кришевич (кримінально-правова характеристика предмета шахрайства, 2012 р.) [56] та інші. Проте у вітчизняній кримінології спеціальні дисертаційні та / або монографічні дослідження шахрайства у сфері електронної торгівлі науковцями не були проведені.

Виходячи з цього, вважаємо, що поширення електронного комерційного шахрайства і вдосконалення інструментарію його вчинення зумовлює необхідність розробки заходів запобігання шахрайству у сфері електронної торгівлі.

1.2. Особливості шахрайства у сфері електронної торгівлі в Україні та світі

Перш ніж перейти до кримінологічної характеристики шахрайства у сфері електронної торгівлі зупинимося на таких явищах, як електронна комерція й електронна торгівля.

Нагадаємо, що між розвитком інформаційного суспільства, а саме ІКТ, та розвитком економіки існує причинно-наслідковий зв'язок, який увібрав в себе, майже, всю історію людства.

Як уже наголошувалося, у світі відбулося декілька інформаційних революцій, у результаті яких вдосконалювалися існуюча, або попередня, форма поширення інформації, у тому числі змінено матеріальні носії інформації. Однак на цей час серед учених не існує одностайної думки щодо кількості таких революцій; хоча залежно від того, появу яких саме способів передачі та/або зберігання інформації вони вважали вирішальними у формуванні інформаційної культури, налічують від чотирьох до шести. Ми ж дотримуємося позиції, згідно з якою людство пережило чотири інформаційних революції [57, с. 41]. Зупинимося на цьому детальніше.

Так, у результаті першої інформаційної революції було винайдено писемність, тобто спосіб передачі інформації; другої – створено книго

друкарні (XVI ст.), третьої – відкрито електроенергію, що, з одного боку, сприяло розвитку різних галузей народного господарства, шляхом створення нових технологій виробництва, а з іншого – забезпечило можливість швидкої та оперативної передачі інформації на значні відстані; четвертої – розроблено мікропроцесорну техніку й персональні комп'ютери (70-ті рр. XX ст.). З огляду на це діяльність окремих галузей і сфер економіки спрямувалася на задоволення інформаційних потреб [58, с. 101]. Іншими словами, четверта інформаційна революція заклала фундамент формуванню електронної комерції.

Концепція електронної комерції була розроблена у Сполучених Штатах Америки (далі – США) ще в 60-х рр. XX ст. для замовлення авіаквитків, обміну інформацією між транспортними службами та координації діяльності служб у процесі підготовки рейсів тощо. Оскільки в ті часи значно збільшився обсяг інформації, яку потрібно було якісно, точно і своєчасно обробляти, згаданий період можна схарактеризувати як час активної трансформації індустріальної робочої сили в інформаційну. Таким чином, у 1964 р. авіакомпанія American Airlines створила систему автоматизованого резервування квитків на авіарейси, яка отримала назву Semi-Automatic Business Research Environment (далі – SABRE). Обмін інформацією в SABRE відбувався через окрему мережу на основі різних стандартів і протоколів, у яких містилися правила електронного оформлення типових ділових документів: замовлень, накладних, митних декларацій, страхових форм, рахунків та ін. На початку 70-х рр. XX ст. в американських компаніях авіаційного, залізничного й автомобільного транспорту функціонувало орієнтовно чотири подібні системи обміну даними. Поступово схожі стандарти обміну з'явилися й в інших країнах. Наприклад, у Великій Британії розроблено серію стандартів і конвенцій по передачі структурованої цифрової інформації між організаціями Tradacoms та General-purpose Trade Data Interchange (далі – GTDI), прийняту Європейською економічною комісією ООН як стандарт обміну даними в міжнародних торговельних організаціях [59]. Пізніше, у 80-х рр. XX ст., на базі

GTDI сформовано Electronic Data Interchange for Administration, Commerce and Transport (далі – EDIFACT, ISO 9735) – бізнес-стандарт оброблення й обміну даними, створений для ефективної взаємодії бізнес-партнерів із метою передачі комерційних даних у вигляді стандартизованих документів з однієї комп'ютерної системи до іншої. Переваги EDIFACT такі: 1) економічність – зменшення витрат на персонал і паперовий документообіг; 2) оперативність – скорочення часу на обробку й передачу інформації від одного бізнес-партнера до іншого; 3) точність – зменшення кількості неточностей та помилок.

У 1981 р. компанія Thomson Holidays UK створили першу бізнес-систему онлайн-шопінгу, а в 1982 р. французький телекомунікаційний оператор France Telecom розробив сервіс онлайн-замовлень Minitel. Очевидно, що справжнім прогресом у сфері торгівлі стало створення роздрібного онлайн-шопінгу Gateshead SIS / Tesco (1984 р.). Таким чином, у 1985 р. Nissan UK почали інтернет-продаж автомобілів. До того ж перший електронний торговий рахунок SWREG видали у 1987 р., а у 1990 р. Тім Бернерс-Лі з колегою Робертом Кайо створили перший вебсайт.

У цілому можна вважати, що розвиток електронної комерції розпочався у 90-х рр. XX ст. з впровадженням у повсякденне життя людей глобальної мережі Інтернет та всесвітньої інформаційно-пошукової системи Word Wide Web (скорочено: WWW). У цей період розроблено новий стандарт EDIFACT over Internet (EDIONT), що сприяло збільшенню оборотів електронної комерції через можливість міжкомп'ютерного обміну комерційними даними у стандартизованому вигляді (або EDI-транзакції).

Враховуючи вищесказане, можемо стверджувати, що глобальний розвиток мережі Інтернет сприяв створенню онлайн-магазинів, які відразу ж стали популярними. Для прикладу, у 1992 р. Book Stacks Unlimited розробили сайт з продажу книг; у 1995 р. Джефф Безос заснував Amazon – майданчик онлайн-продажу універсальних товарів, а Пр'єр Омідьяр – електронний аукціон eBay; у

1998 р. PayPal запустили систему онлайн-платежів; а Google зайнявся електронною комерцією, світовий об’єм якої досяг 8 млрд дол. США за рік.

На початку 2000-х років електронна комерція почала набирати потужність, кількість споживачів, які здійснювали покупки онлайн, складала 50 % від загальної кількості. У цей період Amazon розробили сайт мобільної комерції (2001), Apple почали онлайн-продаж музики через iTunes (2003). Крім того, важливо підкреслити, що між розвитком електронної комерції та продажем iPhone з вбудованим веббраузером (починаючи з 2007 р.) існує двосторонній зв’язок. Так, у результаті постійного розвитку технологій протягом десяти років у 2012 році загальний обсяг продаж електронної комерції перевищив 200 млрд дол. США, а у 2016 році її обороти збільшилися на 45 % у порівнянні з 2015 р. і складали 327 млрд дол. США [60].

Розглянувши генезис електронної комерції, перейдемо до її визначення. У цілому існує безліч підходів до трактування понять «електронна комерція» і «електронна торгівля», як-от: **економічний, юридичний, бізнесовий, маркетинговий**, однак вони носять **описовий, несистематизований характер**.

Поняття «електронна комерція», «електронний бізнес» і «електронна торгівля» досліджувалися багатьма вченими, серед них: В. Тріз, Л. Стюарт [61], А. Брайан Гарднер [62], Я. Задвірний, А. Орловська [63], М. В. Маркова [64], Н. С. Меджибовська [65], В. Л. Плескач [66], А. Маєвська [67], В. С. Мілаш [68]. Однак єдності думок щодо їх визначення досягнуто не було. Відсутність розмежування змісту таких дефініцій в економічній та юридичній літературі, а також неуніфікованість орфографії призводила до того, що фахівці допускали певні неточності у їх трактуванні й застосуванні. Очевидно, що згадані вище поняття необхідно розрізняти [69, с. 56].

Передусім зауважимо, що під **електронним бізнесом** слід розуміти усі форми світових бізнес-процесів, корпоративних додатків, ділових угод, трансакцій, необхідних для створення високоприбуткової та ефективної

моделі електронного бізнесу в будь-якій сфері електронної економічної діяльності, пов'язаної з комерційними операціями організацій і фізичних осіб, а також електронною або мобільною торгівлею [61, с. 34].

Надалі відмітимо, що перше ґрунтовне дисертаційне дослідження електронної комерції було проведене Н. О. Дмітрієвою (2018). Учена **електронну комерцію** визначила як повний цикл міжнародних або внутрішніх бізнес-процесів (господарських операцій), пов'язаних із безпосереднім отриманням прибутку, а також усі форми комерційних угод, трансакцій між її суб'єктами (іноземними покупцями, споживачами, виробниками, продавцями, посередниками, державними органами, фінансовими установами, фізичними особами), які здійснюються в електронний спосіб у будь-якій сфері економічної діяльності й засновані на обробці й передачі цифрової інформації, включаючи тексти, звуки й візуальні дані.

Функціонування електронної або мобільної комерції включає:

1) купівлю-продаж товарів, послуг, інформації; електронні закупівлі як на міжнародних, так і на внутрішніх ринках;
2) будь-які торгові правочини на постачання або обмін товарами чи послугами; дистриб'юторські правочини; комерційне представництво й агентські відносини; використання переважно електронних факторингу, лізингу, консалтингу, інжинірингу; правочини (ліцензійні й про експлуатацію або концесії); договірне оформлення спільних підприємств та інших форм промислового або комерційного співробітництва; адміністрування міжнародних комерційних торговельних операцій (дозвіл, податки, митниця);
3) широке застосування електронних фінансових операцій, а саме: банківських (e-banking); страхових (e-insurance); здійснення операцій з фінансовими інструментами – інтернет-трейдінг (internet trading); обіг електронних грошей (E-cash); електронний рух капіталу (Electronic

Funds Transfer, EFS); використанням відповідних ресурсів Інтернет, Інтранет та Екстранет;

4) процеси формування і стимулювання комерційного попиту; супроводу укладання й виконання угод, адміністративних процедур, пов'язаних з прийняттям і обробкою замовлень; виконання законодавчих вимог, які висуваються до дистанційних комерційних угод, а також автоматизованого обміну інформацією між контрагентами, їх партнерами, постачальниками й клієнтами;
5) електронний маркетинг і електронну рекламу; застосування систем сприяння продажам – передпродажна робота включаючи післяпродажні послуги й підтримку обслуговування покупців; комерційні операції (замовлення, одержання, оплата); автоматизація адміністративних функцій, пов'язаних з електронними продажами й обробленням замовлень; вдосконалення електронного обміну інформацією між партнерами (Electronic Data Interchange, EDI) [70, с. 132].

Говорячи про законодавче визначення, слід звернути увагу на те, що вперше поняття «електронна комерція» нормативно закріплювалося у Комюніке Європейської комісії від 18 квітня 1997 р. «Про Європейську ініціативу в секторі електронної комерції» і встановлювалося, що її основою є електронна обробка й передача даних, яка охоплює електронну торгівлю товарами та послугами, онлайн-постачання цифрового контенту, електронні перекази коштів, електронну торгівлю акціями та державні закупівлі. До того ж згідно з нормами Комюніке електронна комерція поділяється на непряму (електронне замовлення матеріальних товарів, які необхідно доставити фізично, і, відповідно, їх доставка, яка залежить від значної кількості зовнішніх факторів, таких як: ефективність транспортної системи або роботу пошти) і пряму (онлайн-замовлення, яке включає оплату, доставку нематеріальних товарів та/або послуг) [71]. Разом із цим Світова організація торгівлі (далі – СОТ) електронну комерцію визначала як сукупність процесів

щодо виробництва, розповсюдження, маркетингу, продажу й доставки товарів або послуг електронними засобами [72].

Урешті-решт, зосередимо увагу на електронній, або як її ще називають, дистанційній, віддаленій, високочастотній, мобільній торгівлі. Відмітимо, що у Резолюції Генеральної Асамблеї ООН від 16 грудня 1996 р. № A/51/628 «Типовий закон про електронну торгівлю», прийнятій Комісією ООН з міжнародної торгівлі (ЮНСІТРАЛ), поняття «електронна торгівля» прямо не розкривається, проте зазначається, що **електронна торгівля** поширюється на всі відносини комерційного характеру, які здійснюються шляхом обміну інформацією, створеною, надісланою, отриманою і збереженою електронними, оптичними чи схожими засобами, включаючи, але не обмежуючись, електронним обміном даними (далі – EDI), електронною поштою, телексом або телефаксом і застосовується в межах наступних правочинів: будь-які торгові правочини на постачання або обмін товарами чи послугами, дистриб'юторські правочини, комерційне представництво й агентські відносини, факторинг, лізинг, будівництво промислових об'єктів, консалтинг, інжиніринг, ліцензійні правочини, інвестування, фінансування, банківські послуги, страхування, правочини про експлуатацію або концесії, договірне оформлення спільних підприємств та інших форм промислового й ділового співробітництва, правочини на перевезення товарів і пасажирів повітряним, морським, залізничним або автомобільним транспортом [73]. Інакше кажучи, електронна торгівля базується на програмованих повідомленнях, суттєвою відмінністю яких від традиційних паперових документів є їх комп'ютерне програмування.

Крім наведеного, варто зазначити, що правове забезпечення діяльності електронної торгівлі розвивається, проте не такими швидкими темпами як вона сама. Наприкінці XX ст. у зв'язку зі стрімким розвитком ІКТ у країнах-членах ЄС виникли потреби розробки стратегії побудови інформаційного суспільства й нормативно-правового регулювання підприємницької діяльності, яка повністю

або частково здійснюється через телекомунікаційні мережі й Інтернет. У цьому напрямі країни – члени ЄС прийняли значну кількість нормативно-правових актів, які, по суті, спрямовані на створення цивілізованого електронного ринку на європейському просторі й дотримання основних прав, свобод і законних інтересів суб'єктів даних правовідносин, визначених у положеннях Європейської конвенції про захист прав людини і основоположних свобод [74, с. 8]. Серед них варто згадати, зокрема, такі, як: Директива 91/250/ЄЕС Ради Європейського співтовариства «Про правову охорону комп'ютерних програм» від 14.05.1991 р. [75], Директива 97/7/ЄС Європейського парламенту та Ради «Про захист прав споживачів в дистанційних контрактах» від 20.05.1997 р. [76], Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» від 15.12.1997 р. [77], Директива 2000/31/ЄС Європейського парламенту та Ради «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку» від 08.06.2000 р. [78] та ін.

В Україні законодавство у сфері електронної комерції та електронної торгівлі ґрунтується на Конституції України [79] і складається із Цивільного [80] і Господарського кодексів України [81], законів України «Про захист прав споживачів» [82], «Про рекламу» [83], «Про електронні документи та електронний документообіг» [84], «Про захист інформації в інформаційно-телекомунікаційних системах» [85], «Про телекомунікації» [86], «Про електронні довірчі послуги» [87], «Про платіжні послуги» [88], «Про фінансові послуги та державне регулювання ринків фінансових послуг» [89], «Про захист персональних даних» [90], міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

Спеціальний закон про електронну комерцію, який регулює правові відносини у сфері електронної комерції під час вчинення електронних правочинів, в Україні було прийнято 03.09.2015 р., в якому, до речі, й надано визначення поняттям «електронна комерція» й «електронна торгівля».

Так, **електронна комерція** – це відносини, спрямовані на отримання прибутку, що виникають під час вчинення правочинів щодо набуття, зміни або припинення цивільних прав й обов'язків, здійснені дистанційно з використанням інформаційно-комунікаційних систем, внаслідок чого в учасників таких відносин виникають права й обов'язки майнового характеру (ст. 3).

У той самий час, **електронна торгівля** – це господарська діяльність у сфері електронної купівлі-продажу, реалізації товарів дистанційним способом покупцю шляхом вчинення електронних правочинів із використанням інформаційно-комунікаційних систем (ст. 3) [91].

Однак переважна більшість учених піддають критиці вищезгадані законодавчі визначення, пояснюючи це тим, що при розробці проєкту закону законодавцем не були враховані теоретичні розробки економістів, як наслідок, дефініції не мають логічного змісту, що спричиняє численні суперечності й запитання.

Для досягнення мети нашого дослідження варто зупинитися ще на одному моменті: **моделях електронної комерції**. Зокрема, Н. Л. Писаренко виокремлює наступні:

1) **бізнес – бізнес** (business – to – business, B2B) – комерційна взаємодія між бізнесовими компаніями (підприємствами): виробниками, оптовими посередниками, оптовими клієнтами щодо здійснення оптових закупівель та постачання товарів;
2) **бізнес – держава** (business – to – govement, B2G) – ділові зв'язки комерційних структур з державними організаціями, інакше кажучи, проведення державних закупівель через мережу Інтернет;
3) **бізнес – споживач** (business – to – consumer, B2C) – електронна роздрібна торгівля та інші аспекти взаємодії зі споживачем; тобто комерційна взаємодія між електронним магазином і покупцем – безпосереднім споживачем товару;

4) **споживач – споживач** (consumer – to – consumer, C2C) – взаємодія споживачів щодо обміну комерційною інформацією з питань придбання товару чи співпраці з певною фірмою або роздрібна торгівля між фізичними особами;
5) **споживач – держава** (consumer – to – government, C2G) – організація взаємодії між споживачами й державними структурами, особливо в соціальній та податковій сферах;
6) **співробітник – співробітник** (employee – to – emploee, E2E) – організація взаємодії між співробітниками через електронні ресурси: форуми, канали, закриті групи в соціальних мережах чи месенджерах;
7) **бізнес – співробітник** (business – to – employee, B2E) – управління персоналом, формування бренду роботодавця через електронні ресурси компанії [92, с. 352].

При дослідженні шахрайства у сфері електронної торгівлі найбільш вразливими моделями виявилися бізнес – споживач (business – to – consumer, B2C) та споживач – споживач (consumer – to – consumer, C2C).

Певна річ, що ринок електронної торгівлі у наш час активно розвивається не залежно від світових економічних криз чи інших негативних явищ. Так, світовими лідерами за об'ємами електронної торгівлі є Китай, США, Велика Британія та Японія. У цілому Азійсько-тихоокеанський регіон – найбільший ринок електронної торгівлі у світі, в якому темпи росту онлайн-продажів більш ніж на 10 % перевищують середній показник у світі [93]. Нині у світовому рейтингу інтернет-магазинів роздрібної торгівлі за відвідуваністю лідирує Amazon – гігант електронної комерції з Сіетла, який пропонує електронну роздрібну торгівлю, комп'ютерні послуги, побутову електроніку й цифровий контент, зареєстрував у червні 2020 року понад 5,2 мільярда унікальних відвідувачів. Однак за валовою вартістю товарів (GMV) Amazon посідає третє місце після Китаю, конкуренти Taobao і Tmall. Обидві

платформи управляються Alibaba Group, провідним постачальником онлайн-торгівлі в Азії [94].

Водночас до каналів електронної торгівлі можна віднести не лише інтернет-магазини й великі майданчики-маркетплейс, а й соціальні мережі. За інформацією Digitalthirdcoast.com: 1) 40 % продавців використовують соціальні мережі для збільшення кількості продажів; 2) у 2019 році 30 % покупців заявили, що готові купувати товари в соціальних мережах; 3) близько 66 % компаній з більш ніж 100 співробітниками використовують Twitter як частину свого маркетингу; 4) інтернет-магазини з присутністю в соціальних мережах мають на 32 % більше продажів, ніж ті, у кого їх немає. Як ілюстрацію використаємо дані Broadband Search, відповідно до яких онлайн-користувач щодня проводить у соціальних мережах у середньому майже 2,5 години (це 144 хв). Можемо стверджувати, що широке охоплення користувачів, активна діяльність блогерів-провідників думок і рекламно-орієнтований алгоритм роботи цих майданчиків зробили соціальні мережі лідерами електронної торгівлі [95]. Для порівняння візьмемо Facebook з аудиторією близько 2,45 млрд активних користувачів. За допомогою інструментів реклами й Facebook Pay соціальна мережа перетворилася на площадку онлайн-торгівлі. Разом із цим у 2021 році 78 % брендів та ритейлерів використовують пости в Instagram для продажу товарів і послуг.

В Україні за даними проєкту Kantar CMeter до рейтингу популярних сайтів за 2022 рік увійшло чимало маркетплейс й інтернет-магазинів, серед них: Rozetka.com.ua – на 3 місці, Olx.ua – на 6 місці, prom.ua – на 7 місці [96]. Загальновідомо, що Rozetka.ua – найбільший український інтернет-магазин та маркетплейс; Olx.ua – платформа онлайн-оголошень, яка об’єднує людей для покупки, продажу, обміну товарами та/або послугами [97]; prom.ua – український маркетплейс, проєкт IT-компанії, на його платформі підприємці самостійно створюють інтернет-магазини та/або розміщують свої товари в загальному каталозі [98]. Станом на 2018 рік на Olx.ua було зареєстровано 1,5

млн продавців, розміщено понад 11 млн оголошень, а кожну хвилину додається близько 100 нових.

Як ми бачимо, після появи Інтернету, завдяки триваючій цифровізації сучасного життя споживачів, стався зсув попиту від звичайної роздрібної торгівлі до електронної, яку можна назвати ліберальною. Сучасний споживач обирає швидкий спосіб покупки в інтернет-магазині, при цьому маючи можливість порівняти ціни й інформацію про товар на різних сайтах. У той час магазини, які працювали раніше тільки в офлайні, почали освоювати Інтернет.

До того ж у наш час коронавірусна криза (або ж пандемії COVID-19) прискорила розвиток електронної торгівлі. У 2019 – 2022 рр. більш ніж половина населення Землі зіткнулася із карантинними заходами, включаючи локдауни, обмеження пересування, роботи закладів громадського харчування (барів, ресторанів, кафе та ін.), торгово-розважальних і дитячо-розважальних центрів всіх форм власності, закладів розважальної діяльності, роботи непродовольчих ринків/павільйонів, ярмарків тощо. Характерно, що такі жорсткі заходи були впроваджені вперше в історії та призвели до масштабного переходу торгівлі та сфери послуг в онлайн-режим. За даними світових експертів прогнозується зростання об’ємів онлайн-продажів майже втричі протягом 7 років. Зокрема, завдяки такому масовому переходу в онлайн, рівень розвитку сервісної доставки зріс на 22 % [99]. Разом із цим починаючи з 2016 року обіг мобільної комерції збільшився на 15 %, сьогодні майже дві третини (2/3) всіх електронних продажів здійснюється в смартфоні. Отже, відповідні цифри засвідчують домінуючу роль електронної комерції разом з електронною торгівлею в загальній світовій економіці.

Аналогічним чином під час пандемії COVID-19 кількість транзакцій в електронній торгівлі продовжувала зростати. За даними ACI Woldwide, у липні 2020 року кількість міжнародних трансакцій збільшилася на 19 % у порівнянні з липнем 2019 року. В умовах пандемії значно виріс попит на товари для активного відпочинку (на 12 %), ігри (на 52 %) й товари роздрібної

торгівлі (на 48 %) [100]. За висновками дослідження Gradus Research 2021 року щодо змін поведінки українців через COVID-19, електронна торгівля, яка вибухово підвищилася протягом короно кризи, не збирається зупинятися. Так, 61 % респондентів повідомили, що регулярно купують товари в Інтернеті, найчастіше одяг, взуття, гаджети й засоби гігієни. Також, за даними дослідження, двоє з трьох респондентів поповнюють мобільний зв'язок і сплачують комунальні послуги онлайн, а третина купує квитки на транспорт [101].

Без сумнівів, з появою дистанційного шопінгу цілком закономірно збільшилася кількість запитів на здійснення електронних платежів. Учені у цьому випадку застосовують термін «безготівкове суспільство», тобто суспільство, у якому перевагу надають безготівковій системі розрахунків.

Усе сказане означає те, що серед **переваг електронної торгівлі** можна назвати:

1) широкомасштабне охоплення, що цілком логічно, бо через Інтернет можна розширити пошук бізнес-партнерів, ринки збуту товарів та/або послуг, істотно полегшити проведення ринкових досліджень, а також щонайкраще запропонувати свій товар та/або послуги;
2) зручність і швидкість бізнес-процесів;
3) доступність, оперативність інформації, особливо під час міжнародних операцій, доступ інформації з будь-якої точки без додаткових витрат;
4) доступну ціну – онлайн-магазини шляхом зниження невиробничих витрат можуть запропонувати споживачеві більш низьку ціну;
5) цілодобову доступність ринку;
6) широкий асортимент товарів – споживач одночасно має доступ до всього асортименту товару, який розміщується на сайті;
7) інтерактивність спілкування зі споживачем тощо.

Зупинимося й на **недоліках електронної торгівлі**, серед них:

1) обмеження прав споживачів, оскільки споживач не може перевірити якість товару та/або послуги до моменту їх отримання;
2) низький рівень довіри споживачів до електронної торгівлі через відсутність правдивих й чітких описів товарів та/або послуг, пояснення способів оплати й доставки;
3) незнання правил ведення транснаціонального бізнесу;
4) в окремих випадках відсутність універсальних стандартів, невизначеність ряду юридичних і фінансових питань, зокрема, щодо захисту прав інтелектуальної власності, прав споживачів, оформлення договорів, їх юрисдикції та відповідальності за неналежне виконання, захисту інформації, регулювання криптографії;
5) низький рівень безпеки;
6) загрози шахрайства [102, с. 19].

Таким чином, прискорення науково-технічного прогресу зумовлює не лише прогресивні зміни розвитку електронного сегмента ринкових відносин, а й негативні тенденції розвитку злочинного світу, призводячи до появи нових форм і видів злочинних зазіхань. Це проявляється в тому, що злочинці, організовані групи й злочинні організації все активніше використовують новітні досягнення науки й техніки, застосовують різноманітні комп'ютерні пристрої, інформаційно-обробні технології задля отримання прибутку, шляхом шахрайських дій в електронній торгівлі.

Аналітичні й економічні звіти з даного питання досить невтішні. Тільки підприємці справляються з одним видом шахрайства, як на зміну приходить інший. Останніми роками загальна кількість шахрайських спроб у роздрібній електронній торгівлі зросла втричі у порівнянні з 2017 роком. За даними дослідження Risk.lexisnexis 2019 року за кожен долар, яким заволодів шахрай, є-підприємці зазнали збитків в розмірі 3,13 дол., що на 6,5 % більше, ніж за цей період у попередньому році. Очевидно, що нові ринки електронної

торгівлі, особливо транснаціональні, створюють для шахраїв додаткові можливості. Відповідну позицію підтримує 34 % ритейлерів [103].

З огляду на сказане зауважимо, що в Україні останнім часом склалася судова практика з питань кваліфікації шахрайства, вчиненого у сфері електронної торгівлі за ч. 3 ст. 190 КК України, – **шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки.**

Згідно з науково-практичним коментарем до КК України **незаконні операції з використанням електронно-обчислювальної техніки** – це обманне використання можливостей та засобів такої техніки, пов'язане з умисним введенням (закладанням) в її електронну систему неправдивих (свідомо помилкових) даних, що надає можливість шахраю отримати певну суму чужих грошей [104, с. 357]. Точніше, під незаконними операціями з використанням електронно-обчислювальної техніки слід розуміти операції, спрямовані на заволодіння чужим майном або придбання права на майно, в основі яких лежать обман чи зловживання довірою. При цьому вказану кваліфікуючу обставину утворюють лише ті операції, здійснення яких без використання електронно-обчислювальної техніки неможливе (наприклад, здійснення електронних платежів, інших операцій з безготівковими коштами). У такий спосіб електронно-обчислювальна техніка виступає засобом вчинення злочину, а здійснювані з її використанням операції становлять зміст шахрайського заволодіння чужим майном чи правом на нього. Використання електронно-обчислювальної техніки з метою неправомірного заволодіння чужим майном утворює склад злочину, передбаченого ч. 3 ст. 190 КК України лише тоді, коли винна особа заволодіває чужим майном або правом на нього шляхом обману чи зловживання довірою [105].

Відповідно до науково-практичного коментаря с. 361 КК України до **електронно-обчислювальної техніки** належать:

1) **електронно-обчислювальна машина** – комп’ютер – комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних й інформаційних завдань;
2) **автоматизовані системи** – системи, що здійснюють автоматизовану обробку даних, до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки та зв’язку), а також методи й процедури, програмне забезпечення. До складу автоматизованих систем входить принаймні одна електронно-обчислювальна машина й периферійні пристрої, що працюють на основі такої машини: принтер, сканер, модем, сітьовий адаптер та ін.;
3) **комп’ютерні мережі** – об’єднання кількох комп’ютерів і комп’ютерних систем, взаємопов’язаних і розподілених за фіксованою територією й орієнтованих на колективне використання загальномережних ресурсів. Комп’ютерні мережі передбачають спільне використання ресурсів обчислювальних центрів, запуск загальних програм, що входять до комп’ютерних систем; електронно-обчислювальні машини можуть включати дві чи більше автоматизованих комп’ютерних систем як сукупності взаємопов’язаних електронно-обчислювальних машин, периферійного устаткування і програмного забезпечення, призначених для автоматизації прийому, збереження, обробки, пошуку та видачі інформації споживачам. Комп’ютерні системи можуть бути регіонального і галузевого характеру;
4) **мережі електрозв’язку** – сукупність технічних засобів в споруд зв’язку, з’єднаних у єдиний технологічний процес забезпечення інформаційного обміну (маршрутизації, комунікації, передачі, випромінювання або прийому знаків, сигналів письмового тексту, зображень і звуків або повідомлень будь-якого роду по радіо,

проводових, оптичних або інших електромагнітних системах). До них належать, зокрема, телефонний, телеграфний, телетайпний та факсимільний зв'язок. Предмети мережі електрозв'язку включають телефони, факси, телетайпи, телеграфи, інші апарати, пристрої й обладнання мереж електрозв'язку, призначені для передачі та обміну інформацією [106; с. 768].

Сутність вищевикладеного зводиться до того, що **шахрайство у сфері електронної торгівлі** – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки у сфері електронної купівлі-продажу, реалізації товарів у дистанційний спосіб шляхом вчинення електронних правочинів із використанням інформаційно-телекомунікаційних систем.

У цьому контексті варто зупинитися ще на одному моменті. Важливо, що шахрайство у сфері електронної торгівлі має дві основні складові: психологічну й технологічну.

Психологічна складова відповідного кримінального правопорушення полягає в певному впливі на основні елементи мотивації потенційної жертви та спонуканні до вчинення дій в інтересах шахрая. Це можуть бути: 1) бажання отримати прибуток; 2) швидкий спосіб заробітку; 3) бажання безплатно отримати платні товари та/або послуги; 4) прагнення придбати речі або предмети, які або важко, або неможливо придбати в інший спосіб. Більш детально психологію поведінки жертви електронного комерційного шахрайства розглянемо у наступних підрозділах.

Зі свого боку, **технологічна складова** дозволяє шахраєві в сучасних умовах донести до потенційної жертви необхідну інформацію, забезпечити свою анонімність й безпеку, отримати від жертви гроші, не вступаючи з нею в особистісний контакт.

Серед кримінологів сформувалася гіпотеза, що шахраї, учиняючи кримінальне правопорушення в мережі Інтернет, використовують наступні **інформаційно-технічні засоби**:

1) **WWW**, або «всесвітню павутину», що являє інформаційний простір, де документи та інші вебресурси ідентифіковані за уніфікованим покажчиком ресурсів, пов'язаних між собою за гіперпосиланнями, і можуть бути доступні через Інтернет;
2) **E-mail** (електронна пошта) – спосіб обміну цифровими повідомленнями між людьми з використанням цифрових пристроїв, таких як комп'ютери й мобільні телефони, що робить можливим пересилання даних будь-якого змісту;
3) **BBS** – спосіб спілкування користувачів комп'ютерів через комутовані телефонні мережі, який використовувався до часів поширення кабельних комп'ютерних мереж. Зараз втратив свою популярність;
4) **електронні платіжні системи** й **віртуальні гроші.**

Проте вважаємо, що цей список потрібно ще доповнити такими елементами, як:

5) **соціальні мережі** (Facebook, Foursquare, Google+, imo.im, Instagram, Linkedln);
6) **мобільні месенджери** (WhatsApp, Viber, Skype, Telegram, Facebook Messenger),
7) **онлайн-TV**.

Звертаємо увагу на те, що даний список досить швидко збільшується, оскільки інформаційні технології, електронна комерція, електронний бізнес й електронна торгівля не стоять на місці, розвиваються гіпершвидкими темпами, а шахраї, у свою чергу, ще швидше пристосовуються до інновацій.

При цьому варто підкреслити, що ІКТ можуть стати засобами вчинення шахрайства у сфері електронної торгівлі лише за відсутності:

1) постійного й ефективного контролю за правдивістю наданої інформації, правильністю даних, розісланих електронною поштою та розміщених на електронних дошках оголошень та вебсайтах;
2) дієвої системи обміну інформацією щодо скарг користувачів мережі Інтернет;
3) механізму використання цивільноправових зобов'язань у мережі Інтернет.

На закінчення слід сказати, що розвиток нових форм здійснення торговельних і фінансових операцій, а саме електронної комерції, електронного бізнесу й електронної торгівлі в умовах глобальної інформатизації процесів обігу товарів і послуг, які переважно мають транскордонний характер. зумовило рух шахрайства у віртуальний простір, що не містить територіальних і часових меж. Жертвами такого шахрайства стають не лише фізичні та юридичні особи – споживачі товарів та/або послуг, а й виробники, продавці товарів, виконавці робіт, надавачі послуг різних форм власності.

Шахрайство у сфері електронної торгівлі – нове загально масштабне малодосліджене кримінальне правопорушення з **набором характерних особливостей**, які виокремлюють його, а саме:

1) висока латентність;
2) глобальний характер;
3) вчинення кримінального правопорушення у кіберпросторі та віртуальному часі;
4) велика кількість способів вчинення кримінального правопорушення.

Висновки до розділу 1

Під час вивчення думок вчених встановлено, що сьогодні стан наукової розробленості теоретичних і практичних засад запобігання шахрайству у сфері електронної торгівлі потребує комплексного підходу при виявленні,

припиненні й розслідуванні даного виду злочину, що полягає у вивченні як кримінально-правових, кримінально-процесуальних, так і кримінологічних питань. Разом із тим, не применшуючи ролі й значущості праць науковців, слід зазначити, що більшість питань запобігання шахрайству у сфері електронної торгівлі через різні обставини залишається невирішеною, що не може не позначитися на ефективності правоохоронної діяльності.

Встановлено, що на формування шахрайства у сфері електронної торгівлі вплинули такі чинники: 1) четверта промислова революція; 2) цифрова економіка; 3) глобалізація світового співробітництва та економіки; 4) діджиталізація суспільства; 5) стрімкий розвиток ІКТ і мережі Інтернет; 6) діджиталізація банківського сектору; 7) зміна традиційних функцій грошей; 8) професіоналізація й інтелектуалізація злочинності; 9) трансформація індивідуальної злочинності в організовані форми; 10) корпоратизація злочинності.

Наголошено, що електронна торгівля в Україні перебуває на стадії розвитку, що створює сприятливі умови для вчинення шахрайства у цій сфері.

Також за результатами аналізу походження досліджуваного явища сформульовано визначення поняття «шахрайство у сфері електронної торгівлі» – заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки у сфері електронної купівлі-продажу, реалізації товарів дистанційним способом завдяки вчиненню електронних правочинів із використанням інформаційно-телекомунікаційних систем. Визначено такі його ознаки: 1) висока латентність; 2) глобальний характер; 3) вчинення кримінального правопорушення у кіберпросторі й віртуальному часі; 4) велика кількість способів вчинення кримінального правопорушення.

Заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою у сфері електронної торгівлі сприяє виникненню нових загроз стабільного розвитку світової економіки й суспільних відносин у цілому. З огляду на це існує нагальна необхідність консолідації зусиль правоохоронних

органів і розробки наукових рекомендацій щодо вдосконалення практики протидії й запобігання злочинності з метою скорочення її обсягів у державі.

РОЗДІЛ ІІ
ШАХРАЙСТВО У СФЕРІ ЕЛЕКТРОННОЇ ТОРГІВЛІ ЯК ОБ'ЄКТ КРИМІНОЛОГІЧНОГО ДОСЛІДЖЕННЯ

2.1. Кримінологічна характеристика шахрайства у сфері електронної торгівлі

Починаючи висвітлення питання, зауважимо, що сьогодні кримінологи шахрайство умовно поділяють на традиційне (або загально кримінальне) й сучасне. На думку Г. М. Чернишова, під **традиційним шахрайством** необхідно розуміти прості форми обману й зловживання довірою, вчинені поза сферою економіки, які в кримінології відносять до загально кримінальної корисливої злочинності. До таких злочинів учений зараховує карткове, шлюбне (любовне) шахрайство, циганський обман, шахрайство при купівлі-продажу, гральне шахрайство тощо [107, с. 42].

У попередніх підрозділах роботи ми вказували, що **сучасне шахрайство** гіперболізується і проявляється у нових формах. Зокрема, у літературі можна зустріти наступні конструкції: фінансове, банківське, кредитне, корпоративне, інвестиційне, страхове, туристичне, благодійне, комерційне, інтернет-шахрайство, шахрайство у сфері економіки, шахрайство у сфері бізнесу та ін.

Разом із тим як традиційне, так і сучасне шахрайство належать до кримінальних правопорушень проти власності. Стосовно цього Б. М. Головкін зауважує, що кримінальні правопорушення проти власності, пов'язані з незаконним обертанням чужого майна на користь винного чи інших осіб, належать до корисливої злочинності й становлять основний масив так званої загальнокримінальної злочинності в Україні. За масштабами й темпами поширення в суспільстві вони традиційно посідають перше місце (понад 60 %) у

структурі всієї злочинності, а тому значною мірою визначають криміногенну ситуацію в державі в цілому, демонструють стан майнової й особистої безпеки в ній [108, с. 1].

Як відомо, ґрунтовному кримінологічному дослідженню того або іншого різновиду злочинності передує його характеристика, зокрема, аналіз кількісно-якісних показників, що традиційно розглядаються здебільшого у контексті наукової категорії «кримінологічна характеристика» [109, с. 63].

Сприймаючи кримінологічну характеристику як сукупність певних статистичних показників, які ілюструють тенденції злочинних явищ, можна побудувати ретроспективну і перспективну модель певного виду злочинності. І лише за результатами аналізу якісних показників, які можна отримати при вивченні матеріалів кримінальних проваджень, судових рішень, вироків, думок фахівців, інших джерел інформації та їх імплементації з математичними моделями можна виявити ті або інші детермінанти, які притаманні певній динаміці [110, с. 248].

Нижче розглянемо кримінологічну характеристику шахрайства у сфері електронної торгівлі.

Повертаючись до питань термінології, зауважимо, що у науковій літературі існує досить багато визначень поняття «кримінологічна характеристика». Так, на думку переважної більшості вчених, конкретний зміст кримінологічної характеристики полягає у виявленні всіх ознак, що становлять у своїй сукупності й взаємозв'язку її структуру. Узагальнюючи, вчені виділяють такі групи відповідної структури: 1) кримінологічно значущі ознаки злочину; 2) дані, що розкривають кримінологічну ситуацію (типи таких ситуацій, вчинення злочинів); 3) ознаки, що визначають специфіку діяльності з запобігання злочинам. Таким чином, до першої групи відносять властивості особистості злочинця, мотив і мету кримінального правопорушення, властивості особистості потерпілого; до другої – статистику кримінальних правопорушень, відомості про соціальні умови (обстановку) злочину (суспільно-політичну, соціально-економічну обстановки,

час, географію, соціальне середовище і т. д.); до третьої – причини кримінальних правопорушень, їх наслідки, механізм кримінальних правопорушень, обставини, що сприяють злочинам [111, с. 134]. Зі свого боку І. М. Даньшин зазначав, що кримінологічна характеристика охоплює рівень, коефіцієнти, структуру й динаміку злочинів, опис особистості тих, хто їх вчиняє, мотиви й цілі їх злочинної поведінки [112, с. 8].

Надалі саме останньої наукової позиції ми й будемо дотримуватися. Отже, під час розгляду питання кримінологічної характеристики шахрайства у сфері електронної торгівлі першочергово зупинимося на стані, структурі й динаміці кримінальних правопорушень.

У ході побудови кримінологічної характеристики шахрайства у сфері електронної торгівлі також враховуватимемо деякі зауваження й застереження О. Г. Кальмана, які стосуються об'єктивності й достовірності вихідної інформації статистичного аналізу показників кримінологічної характеристики стану економічної злочинності [113, с. 70]. Серед обставин, що обумовлюють потребу взяти до уваги ці застереження при дослідженні показників шахрайства у сфері електронної торгівлі, можна назвати:

1) відсутність офіційних статистичних даних, котрі характеризували б стан шахрайства та інших кримінальних правопорушень у сфері електронної торгівлі в Україні, що викликає необхідність проведення власного вибіркового емпіричного дослідження, яке апріорі не може охоплювати всі 100 % епізодів злочинної діяльності;
2) як і деякі інші прояви злочинності у сфері економіки, шахрайство у сфері електронної торгівлі характеризується високим ступенем латентності. Це ускладнює оцінку його реального рівня. Чітко й однозначно оцінити чисті виміри латентності шахрайства у сфері електронної торгівлі неможливо. Пропоновані показники рівня латентності засновані на теоретичному й емпіричному аналізі явища, наукових гіпотезах тощо. Так, переважна кількість опитаних нами експертів, а саме 48,1 %, рівень

латентності шахрайства у сфері електронної торгівлі оцінили наступним чином**: на одне зареєстроване кримінальне правопорушення припадає десять і більше незареєстрованих**. Причинами такої великої кількості невиявлених і незареєстрованих електронних комерційних шахрайств співробітники органів прокуратури, Служби безпеки України й Національної поліції України вбачають у: 1) відсутності реальних заявників (потерпілої особи) (16 %); 2) недосконалості законодавства (19 %); 3) високому рівні корумпованості органів державної влади, правоохоронних органів, контролюючих суб'єктів й органів місцевого самоврядування (5 %); 4) недостатній кваліфікації працівників правоохоронних органів (18 %); 5) складності розслідування й отримання доказової інформації (42 %).

3) не підконтрольність українській владі деяких регіонів адміністративно-територіальних одиниць унеможливлює ведення статистичного обліку злочинності на цих територіях, що впливає на розрахунки рівня і структури злочинності;
4) відсутність законодавчого визначення понять «шахрайство у сфері електронної комерції» і «шахрайство у сфері електронної торгівлі» призводить до вибору неоднакових підходів до аналізу таких кримінальних правопорушень різними науковцями й дослідниками.

Враховуючи зазначені обставини, відмітимо, що вихідні дані, отримані у ході будь-якого статистичного дослідження показників злочинності, не можна сприймати як абсолютно достовірні, без помилок і похибок. У наукових кримінологічних дослідженнях поряд з офіційними статистичними даними використовуються матеріали спеціально організованих емпіричних досліджень, які полягають, зокрема, в аналізі матеріалів правоохоронної та судової практики, експертних оцінок, опитуванні правоохоронців, потерпілих і пересічних громадян, контент-аналізі повідомлень у засобах масової інформації (далі – ЗМІ) тощо [107, с. 57–58].

Вивчення особливостей шахрайства у сфері електронної торгівлі в запропонованому дисертаційному дослідженні здійснено на підставі 1) аналізу наявних статистичних даних Генеральної прокуратури України щодо стану шахрайства і пов'язаних з ним кримінальних правопорушень за 2013–2021 рр.; 2) узагальнених результатів вибіркового вивчення 361 вироку, ухваленого судами України у 2011 р. та 2016 – 2021 рр., по кримінальних справах щодо шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки; 3) результатів експертного опитування 78 працівників Національної поліції України, прокуратури України, Служби безпеки України, судів і адвокатури України; 4) результатів анкетування громадян України, проведеного онлайн з використанням Google-форм.

У цілому інформаційна модель злочинності має бути побудована на виявленні її реальних якісних і кількісних характеристик у їх діалектичному взаємозв'язку. Одними з найважливіших показників кримінологічної характеристики як усієї злочинності в цілому, так і окремих її видів, груп, виступають рівень злочинності та рівень судимості.

Рівень злочинності – це абсолютна кількість зареєстрованих злочинів і осіб, які їх вчинили, на певній території за конкретний проміжок часу (за місяць, квартал або рік). Даний показник характеризує злочинність з кількісної сторони, тобто визначає її міру й величину [114, с. 19]. Тоді як **рівень судимості** – це абсолютна кількість злочинів, за якими винесено обвинувальний вирок, і кількість засуджених осіб на певній території за конкретний проміжок часу. Зрозуміло, що рівень злочинності завжди більший за рівень судимості, хоча до рівня судимості часто входять особи, засуджені у звітному періоді за злочини, вчинені ними в попередні роки [115, с. 67].

Розглянемо основні показники загально кримінального шахрайства за ст. 190 КК України.

За офіційними даними Генеральної прокуратури України[3] у період з 2013 по 2021 роки спостерігалася як позитивна, так і негативна річна динаміка змін рівня шахрайства, а кількість зареєстрованих шахрайств дорівнювала: у 2013 році – 47142, у 2014 році – 41963, у 2015 році – 45904, у 2016 році – 46019, у 2017 році – 37014, у 2018 році – 33290, у 2019 – 32358, у 2020 році – 26830, у 2021 році – 23847 кримінальних правопорушень.

Аналіз динаміки шахрайства за ст. 190 КК України демонструє певний приріст у період з 2014 року по 2016 рік (позитивний тренд), а починаючи з 2017 року по сьогодні – негативний тренд. Проте обрахунок питомої ваги зареєстрованих шахрайств до загальної кількості зареєстрованих кримінальних правопорушень вказує на дещо іншу тенденцію.

Так, у 2013 році питома вага зареєстрованих шахрайств до загальної кількості зареєстрованих кримінальних правопорушень[4] склала 8,4 %, у 2014 р. – 7,9 %, у 2015 р. – 8,1 %, у 2016 р. – 7,8 %, у 2017 р. – 7,1 %, у 2018 р. – 6,8 %, у 2019 р. – 7,3 %, у 2020 р. – 7,4 % та у 2021 р. – 7,42 %. Як бачимо, на тлі поступового зниження загальної кількості зареєстрованих випадків шахрайств у 2017 – 2020 рр. зберігається стала тенденція шахрайства в загальній структурі злочинності. Більш того, питома вага (відсоток, %) шахрайства у загальній злочинності зростає починаючи з 2018 р. (табл. 2.1). Крім того, попри досить невелику питому вагу вказаних у таблиці шахрайств у структурі всієї злочинності, відносна стабільність показників рівня зареєстрованих кримінальних правопорушень, пов’язаних із шахрайством, свідчить про важливість вивчення шахрайства й шахрайства у сфері електронної торгівлі, зокрема, причин та умов їх існування.

---

[3] Статистична інформація Генеральної прокуратури України про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 15.04.2022).

[4] Відповідно до статистичної інформації Генеральної прокуратури України про зареєстровані кримінальні правопорушення та результати їх досудового розслідування, кількість зареєстрованих кримінальних правопорушень в Україні у 2013 році склала 563560, у 2014 р. — 529139, у 2015 р. — 565182, у 2016 р. — 592604, у 2017 р. — 523911, у 2018 р. — 487133 , у 2019 р. — 444130, у 2020 р. — 360622 , у 2021 р. – 321443. На основі цих показників було здійнено підрахунки питомої ваги шахрайств у структурі всієї злочинності.

Таблиця 2.1

Рівень шахрайства в Україні за 2013 - 2021 рр.

ПОКАЗНИКИ	РОКИ								
	2013	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Кількість облікованих кримінальних правопорушень (крим. правопорушень)	47142	41963	45904	46019	37014	33290	32358	26830	23847
Питома вага зареєстрованих шахрайств у загальній кількості зареєстрованих крим. правопор-нь (у %)	8,4	7,9	8,1	7,8	7,1	6,8	7,3	7,4	7,42

Як зазначалося у попередньому розділі, шахрайство у сфері електронної торгівлі слідчо-судові органи переважно кваліфікують за ч. 3 ст. 190 КК України – шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Отже, нижче розглянемо цифрові показники цього кримінального правопорушення (табл. 2.2), ураховуючи, що для реального встановлення рівня злочинності необхідно брати до уваги два кількісні показники: кількість вчинених кримінальних правопорушень й осіб, які їх вчинили.

Кількість зареєстрованих шахрайств, учинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки у 2013 році становила 3344, у 2014 році – 2760, у 2015 році – 3636, у 2016 році – 3611, у 2017 році – 4845, у 2018 році – 3366, у 2019 році – 2467 кримінальних правопорушень.

Дослідження частки шахрайств, вчинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки, у загальній кількості шахрайств показало позитивний тренд питомої ваги кримінальних правопору-

Таблиця 2.2

Рівень шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки в Україні за 2013 - 2019 рр.[5]

ПОКАЗНИКИ	РОКИ						
	2013	2014	2015	2016	2017	2018	2019
Кількість облікованих крим. правопорушень	3344	2760	3656	3611	4845	3366	2467
Виявлено осіб, які вчинили крим. правопор-ня (особам вручено повідомлення про підозру) за ч. 3 ст. 190 КК України	1053	1238	1321	886	2112	1120	706

шень поміж всіх зареєстрованих шахрайств починаючи з 2014 року – 6,9 %, у 2015 р. – 7,9 %, у 2016 р. – 7,9 %, у 2017 р. – 13,1 %, у 2018 р. – 10,1 %.

Також статистичні дані Генеральної прокуратури України містять деякі відомості щодо кількості виявлених осіб, які вчинили шахрайство шляхом незаконних операцій з використанням електронно-обчислювальної техніки, – рівень судимості. Проаналізувавши дані, наведені в табл. 2.2, можна зробити невтішний висновок. Так, спостерігається низький рівень притягнення винних до відповідальності. Кількість облікованих кримінальних правопорушень, у середньому, більш ніж у 3 рази перевищує кількість виявлених осіб, які їх вчинили. На наше глибоке переконання, зменшення кількості засуджених за вчинення вищезгаданих діянь не свідчить про зниження рівня цієї злочинності, а навпаки, є

[5] Дані наведено за період з 2013 р. по 2019 р. відповідно до статистичної інформації Генеральної прокуратури України про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Починаючи з 2020 р. у звітах наведена загальна інформація про кількість зареєстрованих кримінальних правопорушень та результати їх досудового розслідування за ч. 2–4 ст. 190 КК України. Вирахувати частку шахрайств, вчинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки неможливо.

прикладом недостатньої ефективності роботи правоохоронних органів, недосконалості тактики проведення оперативно-розшукової діяльності, байдужості населення і професіоналізації злочинності.

Водночас для проведення кримінологічного аналізу шахрайства у сфері електронної торгівлі було вивчено 361 вирок за ч. 3 ст. 190 КК України в період 2011 р.[6], 2016 – 2021 рр., за даними, оприлюдненими в Єдиному державному реєстрі судових рішень.

У ході дослідження виявлено, що до кримінальних правопорушень, кваліфікованих за ч. 3 ст. 190 КК України, належить не лише шахрайство у сфері електронної торгівлі. Тому для мети дослідження кримінальне правопорушення за ч. 3 ст. 190 КК України ми класифікували на: 1) фінансове; 2) банківське; 3) «романтичне»; 4) благодійне; 5) електронне комерційне шахрайство; 6) електронне, з ознаками класичного шахрайства. З них електронне комерційне шахрайство складає 57,8 %; банківське – 26,3 %; фінансове – 11,6 %; електронне, з ознаками класичного шахрайства – 2,1 %; благодійне – 1,8 %; «романтичне» – 0,4 %.

У цьому контексті додаймо, що загальний рівень судимості за шахрайства у сфері електронної торгівлі за останні 6 років виглядає наступним чином (табл. 2.3): за 2011 р. засуджено 4 особи, за 2016 р. – 44 особи, за 2017 р. – 53 особи, за 2018 р. – 37 осіб, за 2019 р. – 1 особу, за 2020 р. – 14 осіб, а на кінець серпня 2021 р. – 27 осіб.

При цьому питома вага зареєстрованих шахрайств у сфері електронної торгівлі у загальній кількості зареєстрованих кримінальних правопорушень за ч. 3 ст. 190 КК України у 2011 р. дорівнювала 25 %, у 2016 р. – 64,7 %, у 2017 р. – 74,6 %, у 2019 р. - 7,1 %, у 2020 р. – 43,8 %, у 2021 р. – 44,7 %, тобто близько половини шахрайств, учинених шляхом незаконних операцій з вико-

[6] Враховуючи, що Закон України «Про електронну комерцію» № 45 набрав чинності з 3 вересня 2015 року, для дослідження нами обрано період з 2016 р. по 2021 рік, та для базового порівняння –2011 рік; оскільки перший вирок, кваліфікований за ч. 3 ст. 190 ККУкраїни, було ухвалено в 2011 р.

Таблиця 2.3

Питома вага шахрайства у сфері електронної торгівлі (ч. 3 ст. 190 КК) в Україні (2011, 2016 - 2021 рр.)[7]

ПОКАЗНИКИ	РОКИ						
	2011	2016	2017	2018	2019	2020	2021
Кількість облікованих крим. правопорушень	4	44	53	37	1	14	27
Питома вага зареєстрованих вироків за шахрайство у сфері електронної торгівлі до загальної кількості зареєстрованих злочинів за ч. 3 ст. 190 КК України (у %)	25	64,7	74,6	57,8	7,1	43,8	44,7

ристанням електронно-обчислювальної техніки, є електронним комерційним шахрайством.

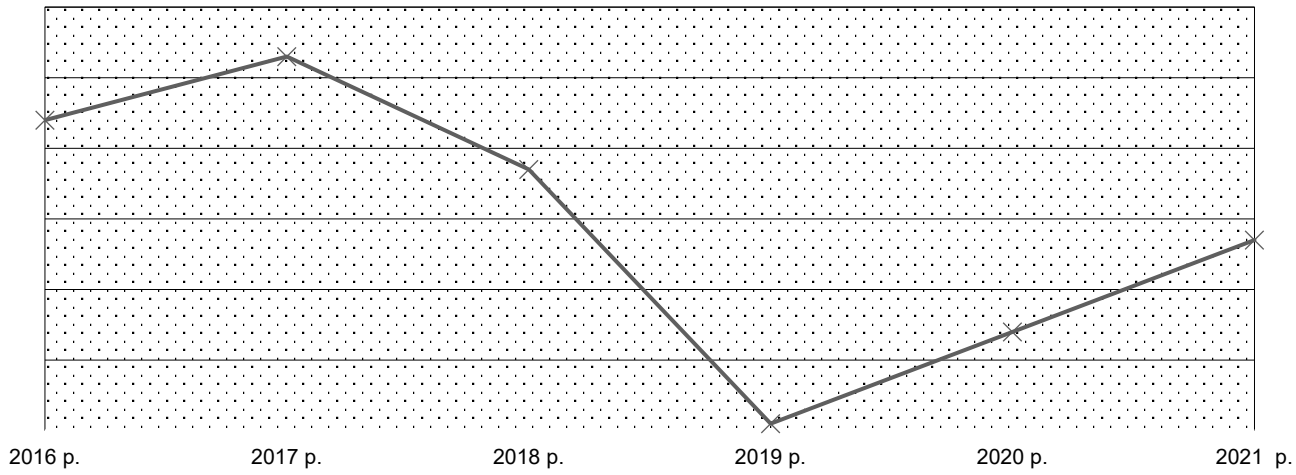
Типовим є те, що для встановлення тенденцій внутрішніх закономірностей розвитку злочинності або її видів необхідно простежити її динаміку за більш-менш тривалий період. Під динамікою злочинності розуміється зміна її рівня і структури за певний проміжок часу в межах певної адміністративно-територіальної одиниці [113, с. 78]. Отже, як ілюстрацію динаміки шахрайства у сфері електронної торгівлі використаємо нижче зображений графік (рис. 2.1).

Характерно, що у 2019 році відмічалося різке зниження кількості зареєстрованих фактів шахрайства у сфері електронної торгівлі. Серед низки детермінант, які безпосередньо вплинули на цей процес, виокремлюємо прийняття Указу Президента України від 14 травня 2020 року №184/2020 «Про введення в дію рішення Ради національної безпеки і оборони України від 14 травня 2020 року «Про застосування, скасування і внесення змін до персональних спеціальних еко-

[7] За даними, оприлюдненими у Єдиному державному реєстрі судових рішень. URL: https://reyestr.court.gov.ua/ (дата звернення: 15.01.2022).

Рис. 2.1

Динаміка шахрайства у сфері електронної торгівлі в Україні за 2016 – 2021 рр.



номічних та інших обмежувальних заходів (санкцій), з зареєстрованим обліковим записом» [116], яким заборонено користування соціальними мережами «ВКонтакт» (URL: vk.com) і «Однокласники» (URL: https://ok.ru) на території України, які до 2019 р. були основним полем діяльності шахраїв.

Зауважимо, що з наведеного графіка спостерігається абсолютний приріст шахрайств у сфері електронної торгівлі. На наш погляд, така позитивна динаміка викликана пандемією COVID-19. Так, у період коронавірусної хвороби у країнах траплялися збої, виникали фінансові проблеми, люди втрачали роботу, суб'єкти господарювання відчули фінансові, операційні й особисті труднощі. Введення карантину, локдауну та інших обмежувальних заходів, дотримання правил соціальної дистанції у відповідь на пандемію COVID-19 призвели до збільшення використання цифрових інструментів комунікації, таких, як соціальні мережі, інтернет-телефонія, телеконференції, а також до фундаментального зрушення у структурі глобального попиту на онлайн-покупки товарів. Іншими словами, у період 2019 – 2021 рр., у буквальному сенсі, відбувся розквіт електронної комерції та електронної торгівлі. Як наслідок, таке електронно-цифрове безпрецедентне середовище, створене пандемією, відкрило нові можливості для шахрайства.

Ведучи мову про особливий віддалений режим електронної торговельної діяльності, варто зауважити, що для електронного комерційного шахрайства не мають значення час і місце вчинення кримінального правопорушення. Зокрема, підозрюваний А., відбуваючи покарання на території Сумської виправної колонії № 116, розташованої за адресою: Сумська область, с. Сад, вул. Войти, 5, діючи умисно, повторно, переслідуючи корисливий мотив особистого збагачення, порушуючи режим відбування покарання, розробив і реалізував план вчинення злочинів, пов'язаних із заволодінням чужим майном шахрайським шляхом – грошовими коштами осіб, які здійснюють роздрібну торгівлю різноманітними товарами через мережу Інтернет, завдяки вчиненню незаконних операцій з використанням електронно-обчислювальної техніки, а також злочинів, пов'язаних із несанкціонованим втручанням в роботу автоматизованих систем ТОВ «Нова Пошта», що призвело до витоку, втрати й підробки інформації[8]. На основі вищенаведеного прикладу можемо констатувати, що шахрай, використовуючи електронно-обчислювальну техніку, може реалізувати свій злочинний умисел у будь-який час доби та з будь-якого місця перебування, навіть відбуваючи покарання у виправній колонії.

У кримінології спосіб вчинення кримінального правопорушення становить значний інтерес, оскільки є основою для формування заходів запобігання. З огляду на це приділимо увагу способам вчинення шахрайства у сфері електронної торгівлі як одній з кримінально-правових ознак.

За результатами проведеного нами опитування через Google-форму, на думку потенційних жертв, заволодіння чужим майном або правом на майно у сфері електронної торгівлі найчастіше вчиняється шляхом: 1) фішингу[9] – 27,56 %; 2) обману або зловживання довірою з авансовим платежем/передплатою – 27,38 %; 3) обману або зловживання довірою з підробкою платіжних квитанцій

[8] Ухвала Київського районного суду міста Харкова. Справа № 953/4432/21. URL: https://reyestr.court.gov.ua/Review/92402919 (дата звернення: 10.10.2021).

[9] Фішинг – сучасний вид шахрайства, спрямований на незаконне отримання даних користувачів: логіна, пароля, платежів, одноразових паролів, іншої інформації з обмеженим доступом.

– 3,37 %; 4) крадіжки персональних даних, злому облікових записів – 13,88 %; 5) обману або зловживання довірою з доставкою – 5,4 %; 6) обману або зловживання довірою з платіжними картами – 11,7 %; 7) обману або зловживання довірою при користуванні мобільними телефонами, зокрема, додатками Google Pay, ApplePay, PayPass – 5,59 %; 8) використання шахрайських платіжних систем – 5,12 %.

Однак вибірковий аналіз судових вироків продемонстрував дещо відмінну картину. Найчастіше електронне комерційне шахрайство пов'язане з отриманням повної (64 %) і часткової (23,3 %) передплат. На одночасне поєднання цих двох форм припадає 4,9 % випадків всіх шахрайств у сфері електронної торгівлі. Більш «рідкими» способами є підміна товару (12 %), фішинг (3 %), крадіжка і використання персональних банківських даних (3 %), а от найменш поширеним вважається вішинг[10] (0,6 %).

До того ж за допомогою нашого емпіричного дослідження вдалося виявити основні майданчики (площадки) шахрайств у сфері електронної торгівлі: aukro.ua, ВКонтакті, Однокласники, Olx.ua, Facebook, Instagram. (табл. 2.4).

Як бачимо, з 2016 р. по 2021 р. найбільше випадків електронного комерційного шахрайства було зареєстровано на сайті Olx.ua; до заборони соціальних мереж ВКонтакті й Однокласники, другою площадкою за кількістю зареєстрованих шахрайств, вчинених у сфері електронної торгівлі, була соціальна мережа ВКонтакті. Пізніше досліджуване кримінальне правопорушення почало переміщуватися у простір інших соціальних мереж – Facebook та Instagram.

Щоправда, за результатами вибіркового аналізу судових вироків нам вдалося виокремили такі категорії товарів і послуг електронної комерції, якими псевдопродавці (шахраї) заманюють жертв (рис. 2.3): 1) транспортні засоби та запчастини до них; 2) косметика і парфумерія; 3) одяг і взуття; 4) оренда нерухомо-

[10] Вішинг - різновид фішингу, при якому також використовуються методи соціальної інженерії, але вже за допомогою телефонного дзвінка.

Таблиця 2.4

Площадки шахрайства у сфері електронної торгівлі у % за 2016 – 2021 рр.

Площадка	2016 рік	2017 рік	2018 рік	2019 рік	2020 рік	2021 рік
Aukro.ua	10 %	6 %	-	-	-	-
ВКонтакті	15 %	17 %	19 %	-	17 %	-
Одноклассники	-	4 %	3 %	-	17 %	-
OLX.ua	60 %	61 %	65 %	100 %	42 %	42 %
Facebook	2,5 %	4 %	6 %	-	8 %	29 %
Instagram	-	-	-	-	8 %	29 %
Інше	12,5 %	8 %	7 %	-	8 %	-

сті; 5) побутова техніка й електроніка; 5) товари загального вжитку.

Рис. 2.3

Предмети посягань шахраїв у електронній торгівлі

Перейдемо до **особи злочинця, який вчиняє шахрайство у сфері електронної торгівлі**.

У цілому у кримінології сформувалися різні підходи до розуміння поняття «особа злочинця».

На думку В. В. Голіни, особа злочинця – це сукупність істотних і стійких соціальних властивостей і ознак, соціально значущих біопсихологічних особливостей індивіда, які, об'єктивно реалізуючись у конкретному вчиненому злочині, надають вчиненому діянню характер суспільної небезпечності, а винній в цьому особі – властивості суспільної небезпечності, у зв'язку з чим вона і притягається до відповідальності, передбаченої кримінальним законом [36, с. 37].

Варто додати, що, розглядаючи корисливу насильницьку злочинність, Б. М. Головкін схематично виокремив три вузлових питання, які підлягають дослідженню при вивченні особи злочинця: а) хто ці люди; б) як вони сприймають соціальну дійсність і ставляться до неї та в якій інтегративній властивості міститься їх криміногенний потенціал; в) у яких формах кримінальної поведінки вони реалізують цю властивість і чому?

Отже, відповіді на ці запитання мають допомогти отримати взаємопов'язані й взаємозумовлені соціально-демографічна, морально-психологічна і кримінально-правова характеристики злочинця [117, с. 119], які, на погляд О. Г. Кальмана, варто розуміти наступним чином:

1) **соціально-демографічна характеристика** – певний статус особи, який визначається її належністю до того чи іншого класу (соціального прошарку) і до групи із соціально-демографічною характеристикою (стать, вік, освіта, сімейний стан, службове становище, національна та професійна приналежність, рівень матеріального достатку тощо);
2) **кримінально-правова характеристика** – спрямованість і характер учиненого злочину, наявність судимості, вчинення злочину у складі організованої групи або злочинної організації, роль у злочинній організації тощо;

3) **морально-психологічна характеристика** – спрямованість особи, система ціннісних орієнтацій, моральні якості особи, її соціальні позиції та інтереси, основні потреби, ставлення до норм моралі, рівень правосвідомості, звички; основні психічні й психофізіологічні особливості; соціальна поведінка, взаємини в колективі, сім'ї, навчальному закладі, найближчому оточенні, а також зв'язки з антисуспільним елементом і самооцінка [113, с. 133].

Таким чином, застосовуючи наведений підхід, на основі результатів експертного опитування працівників Національної поліції України, прокуратури України, Служби безпеки України, судів та адвокатури України, спробуємо встановити типові криміногенні риси осіб, які вчиняють шахрайство у сфері електронної торгівлі.

Аналізуючи **соціально-демографічні ознаки** осіб, які вчиняють шахрайство у сфері електронної торгівлі, виявлено тотальне переважання чоловіків (93,5 %). Частка жінок дорівнює 6,5 %. Таку ситуацію можна пояснити тим, що переважно чоловіки мають аналітичний (математичний або технічний) склад розуму. Жінки, частіше за все, виступають співучасницями таких кримінальних правопорушень.

За ознакою віку розподіл засуджених виглядає наступним чином: 18 – 25 років – 26,1 %; 25 – 35 років – 50 %; 35 – 45 років – 19,6 %; старше 45 років – 4,3 %. З наведених показників вбачається, що переважна більшість (50 %) шахраїв у сфері електронної торгівлі – це працездатні особи віком від 25 до 35 років. У цілому показник віку корелює із рівнем освіти, соціальним статусом, виконуваними ролями, показує соціальну зрілість особистості, життєвий досвід та трудовий стаж.

Освітній рівень шахраїв у сфері електронної торгівлі доволі високий. Зокрема, 27,3 % шахраїв мали повну загальну середню освіту, повну вищу освіту – 25 % шахраїв, професійно-технічну – 22,7 % шахраїв. Базову вищу освіту зафіксовано у 13,6 % злочинців. З базовою загальною середньою освітою налічується 9,1 %, а початковою загальною освітою – 2,3 % засуджених.

За ознакою сімейного стану серед засуджених переважають не одружені/не заміжні особи (57,8 %). Частка осіб, які перебувають у фактичних шлюбних відносинах, становить 22,2 %, одружених/заміжніх – 20 %. Як ми розуміємо, у більшості засуджених не було обов'язку утримувати сім'ю, а відтак дбати про додаткові заробітки, збільшувати фінансові можливості.

За родом занять з-поміж працюючих правопорушників переважають особи з технічною (зокрема, комп'ютерні технології) (65,1 %) й економічною (14 %) спеціальностями. Встановлена тенденція пояснюється тим, що досліджувані злочини можуть вчиняти особи, які вирізняються високими й надвисокими інтелектуальними здібностями (особливо у сфері інформаційно-телекомунікаційних технологій), посидючістю, багатою фантазією і винахідливістю. Досить часто виявляються працівниками банків.

Зрештою, оскільки **кримінально-правові ознаки** особи злочинця проявляються в організації, підготовці й вчиненні окремою особою, організованою групою або злочинною організацією певного кримінального правопорушення, то серед кримінально-правових характеристик шахрая у сфері електронної торгівлі необхідно проаналізувати форму вини, співучасть, вид і розмір покарання.

Як правило, шахрайство у сфері електронної торгівлі характеризуються умисною формою вини. Властивим є прямий умисел, бо шахраї усвідомлюють суспільно небезпечний характер свого діяння, передбачають його суспільно небезпечні наслідки та бажають їх настання (ч. 2 ст. 24 КК України).

Ведучи мову про співучасть в електронному комерційному шахрайстві, констатуємо, що за результатами вибіркового аналізу судових вироків, співучасть слідчо-судовими органами було встановлено лише у 7,3 % кримінальних справах. Такий низький відсоток пояснюється передусім тим, що шахраї добре знають кримінальний закон, зокрема, те, що вчинення відповідного кримінального правопорушення групою осіб за попередньою змовою є кваліфікуючою обставиною, яка збільшує міру відповідальності.

Тому, бувши викритими, винні нерідко заводять слідство в оману стосовно одночасної умисної участі у вчиненні злочину декількох осіб. Крім того, настільки малий відсоток виявлення випадків співучасті, на нашу думку, пояснюється: 1) недостатньою мотивацією працівників правоохоронних органів (низькою зарплатою); 2) небажанням працівників правоохоронних органів виявляти складні кримінальні правопорушення; 3) відсутністю ефективних методів виявлення кримінальних правопорушень; 4) надто великою кількістю роботи.

Відзначимо, що співучасників переважно об'єднують дружні або родинні стосунки, до того ж часто співучасниками злочину стає подружжя. Розглянемо це на такому прикладі[11]. Так, громадянка Б. за попередньою змовою з чоловіком громадянином В. у листопаді 2015 року за місцем свого проживання, відповідно до розробленого й узгодженого між собою плану, розміщували на сайті «http//www.olx.ua» оголошення про продаж побутових товарів з детальним описом та фотографіями, скопійовані з інших аналогічних оголошень у мережі Інтернет, вказуючи ціну, нижчу за середньо ринкову. Подружжя відповідного товару не мало і не планувало замовляти для подальшого продажу. Після виходу на зв'язок особи, яка бажала придбати вказаний в оголошенні товар, переконували її сплатити на вказаний ними картковий банківський рахунок повну передплату вартості замовленого товару, частину вартості або вартість поштової доставки товару. Отримані від замовників гроші подружжя присвоювало та витрачало на особисті потреби, не виконуючи домовленостей. Цікавим у наведеному випадку видається не лише факт співучасті у злочині, а також і процес підготовки до злочину: відкриття банківських рахунків, купівля сім-карт мобільного зв'язку, встановлення спеціальних програм на мобільний телефон для шифрування інтернет-трафіку; а також те, що пропозиція продажу товарів за ціною, нижче

[11] Вирок Індустріального районного суду м. Дніпропетровська. Справа №202/6818/16-к. URL: https://reyestr.court.gov.ua/Review/68093467 (дата звернення: 01.09.2021).

середньо ринкової, виявляється ідеальним «прикормом» для потенційних жертв.

Наприкінці, характеризуючи вид і розмір призначеного покарання за електронне комерційне шахрайство, слід вказати, що найчастіше винним у вчиненні відповідного кримінального правопорушення призначалося умовне позбавлення волі з випробувальним строком (63 %). Основне покарання у виді реального позбавлення волі на строк від 3 до 5 років застосовано у 23 % вироків, рідше призначалися покарання у виді реального позбавлення волі на строк від 6 місяців до 3 років – у 9 % вироків, штрафу – у 4 % вироків, реального позбавлення волі на строк від 5 років та більше – в 1 % вироків. Крім того, існує практика укладення угоди про примирення між потерпілим та обвинуваченим за 2018 р. (справа № 631/138/18) та 2020 р. (справа № 523/19897/20). Як додаткове покарання до основних видів покарань конфіскація майна була призначена судами двічі у 2017 році.

Характерно, що досліджуване кримінальне правопорушення завжди пов’язане із заподіянням матеріальної шкоди жертві. Відповідно до норм ч. 1 ст. 128 Кримінально процесуального кодексу України (далі – КПК) особа, якій кримінальним правопорушенням або іншим суспільно небезпечним діянням завдано майнової та/або моральної шкоди, має право під час кримінального провадження до початку судового розгляду пред’явити цивільний позов до підозрюваного, обвинуваченого або до фізичної чи юридичної особи, яка за законом несе цивільну відповідальність за шкоду, завдану діяннями підозрюваного, обвинуваченого або неосудної особи, яка вчинила суспільно небезпечне діяння [118]. Не відходячи від теми, зауважимо, що за результатами нашого дослідження лише у 2,4 % справ була пред’явлена вимога щодо застосування інституту цивільного позову в кримінальному процесі з метою відшкодування винним заподіяних ним збитків. Такий низький відсоток можна пояснити поганим знанням норм закону, низьким

рівнем правової свідомості та правової культури як потерпілих, так і працівників слідчо-судових органів.

Крім того, у ході нашого дослідження рецидив злочинів встановлено у 35,6 % кримінальних справ, з них у 17,8 % випадків особа вчиняє кримінальне правопорушення, відбуваючи покарання. Вчинення нового умисного кримінального правопорушення особою, яка має судимість за умисне кримінальне правопорушення, свідчить про глибину корисливої спрямованості злочинної поведінки.

Перейдемо до **морально-психологічного** боку особи-шахрая, що охоплює психологічні особливості, інтереси, потреби, соціальні установки й орієнтації, моральні якості, звички особи.

Центральним елементом у системі морально-психологічних ознак винної особи є мотивація дій шахрая, тобто встановлення мотивів вчинення злочину.

За результатами експертного опитування вдалося встановити, що в 50 % випадків шахрайства у сфері електронної торгівлі вчинялися з бажання покращити матеріальне становище, підняти рівень побутового комфорту і створення нових споживацьких можливостей (відпочинок, розваги, престижний одяг, інші витрати), у 26, 9 % випадків – незаконного збагачення у великих й особливо великих розмірах; у 9,6 % випадків – набути високого соціального становища за рахунок постійного джерела незаконних доходів; у 7,7 % випадків – мати додаткові кошти на власні потреби й потреби сім'ї; у 1,9 % випадків – через крайню нужду в елементарних матеріальних благах; у 1,9 % випадків – через необхідність погасити кредити й боргові зобов'язання; у 1,9 % випадків – через безкарність. Отже, оскільки шахрайство належить до групи економічних кримінальних правопорушень, то зрозуміло, що корисливість (користь) є найбільш поширеним його мотивом. Більш детально про корисливість або користь йтиметься в наступних підрозділах.

За результатами дослідження з'ясовано, що типовою особою, яка вчиняє шахрайські дії у сфері електронної торгівлі, переважно є чоловіки, віком 25 –

35 років, які мають середню спеціальну або вищу освіту, досить високий інтелектуальний рівень, мають гарні навички роботи з ІКТ, добре володіють умінням швидко орієнтуватися у ситуації, мають навички психологічного впливу й впевнено користуються довірливістю громадян.

Отже, кримінологічний аналіз шахрайства у сфері електронної торгівлі, має свої особливості через відсутність відображення кримінальних правопорушень в офіційній статистичній звітності й значну їх латентність, що частково ускладнило дослідження. Однак, завдяки вивченню вироків у кримінальних справах щодо шахрайства, встановлено кримінологічно значущі ознаки й характеристики електронного торговельно-комерційного шахрайства і виявлені певні тенденції.

2.2. Причини й умови шахрайства у сфері електронної торгівлі

Шахрайство у сфері електронної торгівлі є наслідком вибору певною частиною суспільства протиправного варіанта поведінки з метою одержання матеріальної вигоди. Ясна річ, існують причини злочинної поведінки, які її породжують, й умови, які сприяють вчиненню кримінальних правопорушень [119, с. 98]. Вочевидь, важливим завданням науки кримінології є глибоке вивчення і розкриття причин й умов злочинності в суспільстві, адже лише на їх основі можлива розробка ефективних заходів запобігання і протидії злочинності.

Передусім зазначимо, що під словом «причини» розуміємо підставу, привід до яких-небудь дій, вчинків або ж явище, яке породжує інше явище (наслідок). Так само, **причини злочинності** – це явища суспільного життя, які не лише породжують злочинність, а й підтримують її існування, викликають її зростання або зниження. Сфера дії причин – це стадія мотивації й ухвалення рішення, коли йдеться про формування мотиву, мети, визначення шляхів її досягнення саме як злочинних [120, с. 46]. Зрозуміло, що між причиною і наслідком існують бінарний (дволанковий) зв’язок або причинний ланцюг. Причина створює можливість певного наслідку, однак для його настання необхідні умови. У цьому контексті

умови злочинності – це явища, які самі не породжують злочинності й злочинів, а сприяють, полегшують, інтенсифікують формування й дію причин. Йдеться про різноманітні явища, процеси, обставини, які сприяють або створюють можливість для виникнення і прояву причин, які породжують наслідок [121, с. 188].

Завданням даного підрозділу є визначення й розкриття причин і умов вчинення шахрайства у сфері електронної торгівлі. Для досягнення поставленої мети використаємо багатофакторний аналіз, що дозволяє зіставити різні групи соціальних факторів у їх взаємодії, виявити взаємозв'язки між ними, провести комплексний аналіз впливу на етіологію злочинності у сфері електронної комерції як криміногенних, так і антикриміногенних факторів, визначити явища і процеси суспільного життя, які потребують більш інтенсивного профілактичного впливу. Вивчаючи фактори кіберзлочинності в Україні, Б. М. Головкін, С. С. Чернявський та О. В. Таволжанський, за змістом і сферами дії детермінанти кіберзлочинності класифікують на глобалізаційні, політичні, економічні, соціокультурні, технологічні, інформаційно-психологічні, нормативно-правові, організаційно-управлінські, віктимогенні, а також чинники, пов'язані з неефективною діяльністю органів правопорядку [122].

У межах нашого дослідження сукупність причин і умов вчинення шахрайства у сфері електронної торгівлі умовно поділяємо на: **соціально-економічні**; **організаційно-управлінські**; **морально-психологічні**. Більш детально розглянемо їх нижче.

До **соціально-економічних** криміногенних чинників пропонуємо віднести:

1) лібералізацію й глобалізацію цифрової економіки;
2) стрімкий перехід торгівлі з офлайн режиму на онлайн, викликаний коронавірусною кризою;
3) низький рівень доходів, обмежену купівельну спроможність громадян, високі показники безробіття;

4) марнотратство, звичку витрачати більше, ніж заробляєш;
5) крайню нужденність у товарах повсякденного життя, дефіцит окремих категорій товарів.

Нагадаємо, що особливостями нинішнього стану економіки є процеси глобалізації та лібералізації. Так, глобалізація – це процес, який передбачає: 1) реорганізацію виробництва у просторі; 2) взаємопроникнення промислових підприємств через державні кордони; 3) розширення фінансових ринків; 4) збільшення частки іноземних прямих інвестицій в економіки, які розвиваються; 5) розширення глобального ринку праці; 6) розповсюдження технологій, міжнародних комунікацій та всесвітньої культурної інтеграції; 7) розповсюдження споживацьких товарів, масові переміщення населення як на Півдні, так і на Сході й Заході [123, с. 4 - 5]. У результаті глобалізації стираються географічні кордони держав, відбувається злам у психосфері особистості, змінюються культурні, психологічні, моральні форми існування людей.

Глобалізація неможлива без процесів лібералізації. У цілому науковці виокремлюють різні напрямки лібералізації, серед них: політичний, соціальний, законодавчий, економічний, який включає валютно-фінансовий, банківський, бюджетний, зовнішньоекономічний, та ін. На думку В. М. Сторожука, основними характеристиками лібералізації є: 1) надання свободи й зняття (усунення, послаблення) обмежень, причинно-наслідковий зв'язок між ними; 2) наділення правом установлення/усунення обмежень окремих суб'єктів управління – інституцій, органів управління, посадових осіб та ін.; 3) набуття суб'єктами управління прав і свобод у сфері їх діяльності, у результаті прийняття рішень [124, с. 26]. До основних принципів економічної лібералізації можна віднести: 1) приватний інтерес, побудований на приватній власності; 2) свободу вибору сфери діяльності; 3) свободу обміну економічними благами; 4) наявність конкурентного середовища без ознак протекціонізму й дискримінації; 5) функціонування ринків ресурсів, вільний, рівноправний доступ до них; 6) фінансову стабільність із прогнозованою

керованою інфляцією; 7) низькі податки; 7) стійкі й ефективні «правила економічної гри» [125, с. 184]. Головне, що економічна свобода, якої набувають господарюючі суб'єкти в результаті лібералізації економіки, виступає визначальним принципом функціонування економічної системи ринкового типу.

Очевидно, що процеси глобалізації та лібералізації економіки вплинули на становлення і розвиток цифрової економіки, що, у свою чергу, переорієнтувало увагу шахраїв на новостворену сферу.

Наступним фактором шахрайства у сфері електронної торгівлі став вплив пандемії COVID-19 на економічну діяльність і соціальну поведінку, що спричинив стрімку трансформацію й організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем [35]. У період обмежень, пов'язаних із коронавірусом, попит з офлайну масово перемістився в онлайн. За словами К. Андерсона, у 2020 р. обсяги електронної торгівлі збільшилися приблизно втричі у порівнянні з показниками 2019 р., вдвічі зріс попит на продукти й товари першої необхідності [126]. Як наслідок, пандемія COVID-19 матиме довготривалий вплив на торгівлю, посилюючи роль електронних комунікацій у повсякденному спілкуванні й роботі, що підвищує ступінь її вразливості, процесів обробки інформації, зокрема, персональних даних.

Аналогічним чином пандемія COVID-19 спровокувала зростання світового рівня бідності. В Україні найвищий показник рівня бідності був зареєстрований у 2000 р. – 71,2 %. Наступні вісім років він поступово знижувався, досягнувши у 2008 р. мінімального значення – 19,9 %. Протягом 2008 – 2013 рр. рівень бідності в Україні то зростав, то зменшувався. Різке погіршення ситуації відбулося з початку російської збройної агресії проти України (табл. 2.5). Так, рівень бідності у 2014 р. становив 28,6 %, у 2015 р. – 58,3 %, у 2016 р. – 58,6 %. Пізніше він почав знижуватися: у 2017 р. – до 47,3

%, у 2018 р. – до 43,2 %; у 2019 р. – до 37,8 %. Проте, як бачимо, пандемія COVID-19 звела нанівець здобутки, які було досягнуто раніше.

Таблиця 2.5

Рівень абсолютної бідності в Україні з 2013 по 2021 рр.[12]

Рік	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Рівень бідності, у %	22,1	28,6	58,3	58,6	47,3	43,2	37,8	43,6	51

Відповідно до звіту, присвяченому глобальному Індексу багатовимірної бідності за 2021 рік[13], який підготували Програма розвитку ООН та Оксфордська ініціатива з питань бідності та людського розвитку, в Україні у багатовимірній бідності живе 0,2 % населення (це близько 107 000 осіб). Масштабність нестатків в Україні співмірна з середніми показниками нестатків серед людей, які живуть у багатовимірній бідності, становить 34,4 % [127].

Бідність – не лише соціальна, а й економічна категорія, а отже, залежить від таких макроекономічних показників, як обсяг валового внутрішнього продукту (далі ВВП), індекс інфляції, рівень безробіття й реальна заробітна плата.

По-перше, попри те, що номінальний ВВП[14] на душу населення в Україні зростає: у 2015 р. – 2115,4 дол. США, у 2016 р. – 2185,9 дол. США, у 2017 р. – 2640,3 дол. США, у 2018 р. – 3095,2 дол. США, у 2019 р. – 3659,8 дол. США, у 2020 р. – 3725,6 дол. [128]; Україна посідає 122 місце в списку країн за ВВП на душу населення. Для прикладу, у сусідніх Польщі ВВП на душу

[12] За даними UNICEF на основі досліджень Держстату та Інституту демографії та соціальних досліджень імені М. В. Птухи

[13] Бідність вимірюється, враховуючи різноманітні нестатки, які відчувають люди у повсякденному житті, включаючи погане здоров'я, брак освіти та низький рівень життя.

[14] Валовий внутрішній продукт (скор. ВВП, англ. Gross Domestic Product, GDP) – макроекономічний показник, що показує ринкову вартість усіх кінцевих товарів і послуг, вироблених за рік у всіх галузях економіки на території держави для споживання, експорту та накопичення, незалежно від національної приналежності використаних факторів виробництва.

населення складає 15,431 дол. США, у Румунії – 12,285 дол. США, у Болгарії – 9,267 дол. США [129].

По-друге, за даними державної служби статистики, у 2020 р. помітне зростання індексу інфляції[15] в умовах пандемії COVID-19 на 1,00 % та у 2021 р. на 2,5 % (табл. 2.6). У цілому індекс інфляції відображає економічну ситуацію в країні.

Таблиця 2.6

Індекс інфляції з 2015 по 2021 рр.

Період	Індекс інфляції, %	Інфляція, %	Зміни
2015 р.	143,30	43,30	+ 18,30 %
2016 р.	112,40	12,40	- 30,60 %
2017 р.	113,70	13,70	+ 1,70 %
2018 р.	109,80	9,8	- 4,20 %
2019 р.	104,10	4,10	- 5,90 %
2020 р.	105,00	5,00	+ 1,00 %
2021 р.	107,50	7,50	+ 2,50 %

По-третє, вплив коронавірусної кризи чітко простежується на сфері зайнятості населення. За словами міжнародних експертів, у світі через коронакризу було втрачено близько двохсот п’ятдесяти (250) мільйонів робочих місць, що вчетверо більше, ніж під час фінансової кризи 2009 року. Без роботи залишилися переважно співробітники готельно-ресторанного бізнесу і сфер послуг. Зайнятість у цих секторах скоротилася в середньому на 20 % [130]. Найбільш складно доводиться молоді віком від 21 до 25 років, які в цей період закінчили вищі навчальні заклади й змушені були шукати роботу. У цілому у 2021 р. рівень зайнятості серед населення віком від 15 до 70 років становить 56,2 %, а рівень безробіття серед робочої сили віком від 15 років і старше дорівнює 9,3 % [131].

[15] Індекс інфляції або індекс споживчих цін — показник, що характеризує зміни загального рівня цін на товари і послуги, які купує населення для невиробничого споживання.

По-четверте, попри те, що в Україні з 1 січня 2022 року підвищили мінімальну заробітну плату до 6 тис. 500 грн, понад чверть усього населення України перебуває за межею бідності, кожному третьому українцю, який має роботу, не вистачає зарплати на задоволення життєвих потреб. Аналогічно, середня номінальна заробітна плата штатного працівника в Україні в червні 2021 року зросла у порівнянні з червнем 2020 року на 23,6 % – до 14 тис. 313 грн, проте станом на серпень 2021 року лише 1% українців вважав себе представниками середнього класу, у той час, як дві третини населення (67 %) віднесли себе до категорії бідних. За результатами проведеного опитування Київського міжнародного інституту соціології, понад 14 % населення України не вистачає грошей навіть на їжу. Лише 32,8 % громадян можуть дозволити собі купувати продукти харчування, одяг і трохи відкладати, але вони не можуть купити дорогу техніку (холодильник або телевізор) [132]. Отже, за 30 років незалежності України купівельна спроможність українців впала на 30 %, а за індексом щастя Україна посідає 110 місце.

Зрозуміло, що в умовах бідності у людей формуються неформальні цінності, девіантні форми поведінки й кримінальні практики.

Також спостерігається тенденція до того, що в епоху глобального розвитку цифрових технологій, маркетингу, електронної комерції та торгівлі стрімко зростає рівень марнотратства споживачів і формується звичка витрачати більше, ніж заробляєш. Так, у зв'язку з активною популяризацією брендів, яскравими рекламними компаніями товарів і послуг, загальнодоступним рівнем життя бізнесменів, моделей та інших знаменитостей, у людей виникає непереборне бажання жити багато й розкішно. Це спричиняє нерозумне витрачання грошей формується звичка купувати модний одягу, взуття, парфуми, аксесуари, електроніку за низькими цінами. У пошуку найдешевших варіантів люди користуються послугами інтернет-магазинів, площадок із продажу вживаних товарів або речей. Характерно, що сучасні шахраї ґрунтовно аналізують ринок електронної

торгівлі та психологію споживача з метою успішного досягнення поставленої корисливої мети.

До групи **організаційно-правових** криміногенних чинників пропонуємо віднести:

1) упровадження нових технологій;
2) недосконаліть законодавства у сфері електронної торгівлі;
3) недосконаліть нормативно-правової бази у сфері кібербезпеки;
4) недосконаліть державного контролю за електронною торгівлею;
5) низький рівень викриття і притягнення до кримінальної відповідальності;
6) низький рівень обізнаності у сфері кібербезпеки громадян.

Як було зазначено вище, нові виклики несе діджиталізація суспільства, а точніше швидкі прогресивні зміни ІКТ, зокрема, хмарних і квантових обчислень, великих даних, інтернет-речей, штучного інтелекту; перехід на 5G-мережі, функціонування яких суттєво залежить від коректної роботи програмного забезпечення, що за рахунок новизни технології може нести нові, не передбачені загрози. Відсутність системи оцінки відповідності продукції ІКТ вимогам безпеки підвищує ступінь уразливості інформаційної інфраструктури від незадекларованих функцій і звужує спроможності протидії кіберзагрозам [35].

Разом із тим проблемним залишається питання недосконалості законодавства у сфері електронної торгівлі. Зазначимо, що закон, який закріплює організаційно-правові засади здійснення електронної комерції в Україні та регулює відносини, що виникають під час укладення й виконання правочинів, вчинених в електронній формі із застосуванням інформаційно-телекомунікаційних систем, був прийнятий 3 вересня 2015 року. Однак вищезгаданий нормативно-правовий акт містить цілу низку суперечностей, із його ухваленням постало більше запитань, ніж отримано відповідей. Більш того, він суперечить Директиві Європейського Союзу «Про електронну

комерцію» і розпорядженню Європейського Союзу щодо електронної ідентифікації та договірних послуг для цілей електронних транзакцій на внутрішньому ринку. До того ж у цьому Законі використовується термінологія, не характерна для Цивільного кодексу України та його положень, що створює ряд юридичних колізій, це стосується, зокрема, і Закону України «Про електронний цифровий підпис» [133, с. 168 - 169]. Очевидно, що наявна нормативно-правова база у сфері електронної купівлі-продажу є недосконалою. Точніше, у Законі «Про електронну комерцію» не врегульовано процедури підтвердження факту купівлі-продажу і підписання договору, некоректно наведені визначення більшості понять предметної сфери електронної торгівлі (електронна комерція, електронна торгівля тощо), відсутній принцип свободи договору, не визначено місце укладення електронного договору. Зрозуміло, що наслідками недосконалості законодавства у сфері електронної торгівлі є: 1) складність визнання транскордонних електронних правочинів (комплексу прав і обов'язків сторін електронного правочину); 2) складність підтвердження наявності взаємовідносин; 3) неналежна імплементація електронних послуг (у тому числі довірчих). До того ж кожна прогалина в законі – це додаткові можливості для злочинця.

Крім того, додаткові передумови та чинники, які формують загрози шахрайства у сфері електронної торгівлі, несе недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства, недостатня урегульованість цифрової складової розслідування кримінальних правопорушень, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері [35].

Не менш загрозливою на даному етапі розвитку є відсутність органу, який відповідає за формулювання й реалізацію державної політики у даній сфері. До речі, це також визнається причиною шахрайства у сфері електронної

торгівлі в Україні, що зумовлює: 1) розпорошеність повноважень регулювання сфери електронної торгівлі між різними органами державної влади; 2) відсутність постійного моніторингу й корегування нормативно-правового регулювання швидкоплинних процесів, зумовлених, зокрема, розвитком ІКТ; 3) відсутність системного підходу до регулювання відповідної сфери; 4) відсутність прийнятного статистичного обліку кількості, якості і структури розгляду скарг споживачів електронної торгівлі, які потребують постійного нагляду і втручання держави [134].

Також до групи організаційно-правових криміногенних чинників слід віднести низький рівень викриття і притягнення до кримінальної відповідальності осіб, які вчиняють шахрайство у сфері електронної торгівлі. Це викликано: 1) відсутністю у значної частини державних органів відповідних структурних підрозділів, необхідного кадрового забезпечення і належного контролю за кіберзахистом; 2) здійсненням фінансування робіт із кіберзахисту за залишковим принципом; 3) невідповідністю сучасним вимогам рівня підготовки й підвищення кваліфікації фахівців із питань кібербезпеки та кіберзахисту, зокрема, неефективні механізми їх стимулювання до роботи в державному секторі. Так само, на думку С. В. Самойлова, складність розслідувань шахрайств із використанням мережі Інтернет пов’язана з тим, що відповідне кримінальне правопорушення є специфічним явищем у сучасній злочинності, оскільки може мати як прояви всередині держави, так і охоплювати території інших держав, набуваючи транснаціонального характеру, а тому фізичне місцезнаходження шахрая, як і засобів учинення злочину, переважно не збігаються з місцем перебування потерпілого і настанням негативних наслідків злочину (місцем завдання матеріальної шкоди), а в певних випадках такі обставини можуть мати навіть транснаціональний (трансконтинентальний) характер [135, с. 12].

На останок зауважимо, що серед організаційно-правових криміногенних чинників варто вказати й відсутність системи підвищення цифрової грамотності

громадян і культури безпекового поводження в кіберпросторі, низький рівень обізнаності суспільства щодо кіберзагроз і кіберзахисту.

До **морально-психологічних** криміногенних чинників ми відносимо:

1) деформацію правових і моральних цінностей, низький рівень правосвідомості й правової культури;
2) перехід від реального спілкування до віртуального;
3) переважаючий емоційний інтелект людей;
4) ігровий характер поведінки;
5) домінування матеріальних цінностей над духовними;
6) неповідомлення жертвами шахрайства про кримінальне правопорушення.

Шахраїв, як і переважну більшість осіб, які вчинили кримінальне правопорушення, вирізняють набір негативних особистісних якостей, деформовані правові й моральні цінності, низький рівень правової культури та правової свідомості.

Чимало вчених морально-психологічні чинники поділяють на зовнішні й внутрішні. Отже, зовнішні морально-психологічні чинники мають соціальну природу і визначаються ставленням соціальних груп до норм традиційної й сучасної моралі, а саме: 1) схвальне ставлення значної частини економічно активного населення до обману і зловживання довірою; 2) переважання у свідомості молоді цінностей грошей, гедонізму, особистого успіху; 3) зневажливе ставлення до чесної праці й до помірного використання матеріальних благ; 4) орієнтація більшості на моральні норми індивідуалізму і прагматизму. Тоді як до внутрішніх (або особистісних) належить: 1) схильність до маніпуляції іншими людьми для отримання особистої вигоди; 2) цінності самозвеличення над людьми; 3) егоїстичне відчуження від інших людей і моральних норм. Інтуїтивно шахраї використовують фактор навіювання, впливаючи на емоції та почуття, тобто на підсвідомість жертви, тим самим маніпулюючи поведінкою, розумом і волею людини незалежно від

рівня освіченості [136, с. 218]. Щодо цього, на наш погляд, цікавою є точка зору Г. М. Чернишова, згідно з якою до соціально-психологічних чинників фінансового шахрайства в інвестиційно-будівельній сфері, так само у сфері електронної торгівлі, належать: 1) споживча ідеологія, культ матеріальних речей і багатства; 2) соціальна аномія; 3) ідеологічна криза, романтизація злочинності [137, с. 125 - 126].

Наведене пояснюється тим, що в умовах масової діджиталізації спостерігається різке зниження загальної культури людей і правової зокрема. Взагалі, правова культура – це якісний стан правового життя суспільства, який характеризується досягнутим рівнем розвитку правової системи — станом і рівнем правосвідомості, юридичної науки, системи законодавства, правозастосовної практики, законності й правопорядку, правової освіти, а також ступенем гарантованості основних прав і свобод людини [138, с. 550].

Так, Л. О. Макаренко узагальнила основні характеристики правової культури. На її погляд, правова культура – це, зокрема: 1) необхідна умова розвитку інтелектуального, духовного потенціалу народу, утвердження цілісної системи світоглядно-ціннісних орієнтацій, передусім сучасного юридичного світогляду, правових ідеалів, праворозуміння; 2) спосіб діяльності й мислення, норми й стандарти поведінки, які містять лише те, що є прогресивним, соціально корисним і цінним; 3) система правових цінностей, які відповідають рівню досягнутого суспільством правового прогресу й відбивають у правовій формі стан свободи, інші соціальні цінності (об’єктивне й суб’єктивне право, правові принципи, правомірну поведінку, законність і правопорядок); 4) ідеї, цінності, очікування й ставлення до права та юридичних інститутів, яких дотримується певне суспільство або певна частина суспільства; 5) різновид культури, зумовлений економічним, політичним, соціальним і духовним рівнем розвитку суспільства, що матеріалізується у формуванні, передачі й збереженні правових цінностей, які є орієнтирами юридично значущої поведінки; якісний стан правової системи, ступінь правового розвитку особистості й суспільства; 6) усвідомлення

конкретною людиною наявної системи права і правових знань, правомірне дотримання їх у своєму житті, що характеризує певний рівень знання права членами суспільства, їх поважне ставлення до нього, престиж права в суспільстві, стан правової свідомості учасників суспільного життя [139, с. 26–28]. Своєю чергою, С. І. Максимов виокремлює три рівні правової культури: 1) рівень правосвідомості, так би мовити, духовно-ментальне ядро, яке включає цінності, ідеали й загальне праворозуміння, що виражається в усвідомленні значущості прав людини, їх обсязі та ступені захищеності; 2) інституційний – рівень розвитку юридичних норм та інститутів; 3) рівень правової діяльності, що складається з теоретичної продуктивної (діяльність учених-юристів) і репродуктивної діяльності (юридична освіта в усіх її формах, видах і настановах), а також з практичної – правотворчої та правореалізуючої, у тому числі правозастосовної діяльності [140, с. 212–213]. Суть вищевикладеного зводиться до того, що низький рівень правової культури й правової свідомості особи переважно виступає морально-психологічним криміногенним чинником шахрайства у сфері електронної торгівлі.

Ще одним морально-психологічним чинником шахрайства у сфері електронної торгівлі, на нашу думку, є перехід від реального спілкування до віртуального. Певна річ, що люди проводять велику кількість часу в мережі Інтернет. За даними дослідження Digital 2020, основна мета якого – показати, що цифрові, мобільні й соціальні медіа стали незамінною частиною повсякденного життя людей у всьому світі; пересічний користувач мережею проводить понад 6 годин 43 хвилини в Інтернеті щодня, що приблизно становить 100 днів на рік [141]. Через це традиційний процес комунікації між людьми кардинально змінився, з’явився додатковий простір для спілкування – віртуальний, у якому зникають просторові й часові розмежування, стираються міждержавні кордони, пропагуються нові цінності, моделі поведінки, світоглядні стереотипи.

Сьогодні у вітчизняній науці питання віртуальної реальності досліджує О. П. Дзьобань. Науковець у численних публікаціях зазначає, що віртуальна реальність, створювана сучасними засобами масової комунікації, формує у свідомості людей ідею використовуваності, тобто людина переконана в тому, що завжди перемагає найсильніший, отримуючи всі преференції від життя, інші ж не мають права претендувати ні на що. Кожен є «сам за себе», вливається в групи лише для того, щоб за допомогою інших людей змогти досягти блага для себе. Мірилом того, якою є людина – доброю чи поганою, стає лише те, перемогла вона чи ні. При цьому перемогою або поразкою вона зобов'язана тільки собі, тільки своїм вірним/невірним вчинкам й особистим якостям. Тому склалася думка, що у цьому світі можна виграти лише те, що програють інші й навпаки [142, с. 74]. Зрозуміло, що під впливом віртуального спілкування змінюється свідомість особистості, формується новий мережевий образ мислення й існування, що, своєю чергою, зумовлює злочинну поведінку.

Крім того, що у результаті стрімкого інформаційно-технологічного прогресу трансформувалася сфера комунікацій, у більшості людей сформувався ігровий характер поведінки. Одним словом, комп'ютер був створений з метою спрощення роботи працівників різних професій, однак через розвиток ІКТ почав використовуватися для проведення за ним вільного часу й різного роду розваг, зокрема, гри в комп'ютерні ігри. Сьогодні питання комп'ютерної залежності посідає чільне місце в науковому середовищі, учені обговорюють вплив комп'ютерних ігор на формування особистості, логічне мислення, психічний стан особи. Так, вітчизняні соціологи О. А. Гульман та Н. О. Ляшенко соціальну небезпеку комп'ютерних ігор вбачають у: 1) збільшенні матеріальних витрат на гру й ризик програшу; 2) уникненні реалій, підміні реального життя нереальним світом гри; 3) формуванні установки на «легку здобич», «халяву»; 4) вірі в фаталізм; 5) підштовхуванні особи до будь-яких шляхів (у тому числі злочинних) отримання необхідних коштів для гри; 6) небезпеці реальних психічних розладів (захворювання на гемблінг –

патологічний азарт) [143]. Тож убачаємо, що переважаючий ігровий характер особи може бути одночасно причиною й умовою шахрайства у сфері електронної торгівлі.

У результаті духовної спустошеності сучасного суспільства, утрати ним духовних цінностей, дегуманізації всіх сторін життя, девальвації загальнолюдських цінностей, непомітної підміни істинних цінностей анти цінностями масової культури, посиленням процесу індивідуалізації, домінуванням ринкових відносин [144, с. 3], активною пропагандою засобами масової інформації розкоші й багатства відбувається прищеплення таких негативних якостей людини, як егоїзм, нахабність і жадібність. В умовах перенасичення ринків товарами й послугами, економічно нестабільної ситуації в державі, змінення сучасними кібертехнологіями свідомості особи та ставлення до грошей, у людей формується хибна життєва позиція – домінування матеріальних цінностей над духовними, що формує та посилює мотивацію до учинення електронного комерційного шахрайства. При цьому, на наш погляд, жадібність одночасно виступає як причиною, так і умовою вчинення відповідного кримінального правопорушення. З цього приводу у суспільстві сформувалася усталена думка, що шахрайство можливе за взаємною жадібністю і дурістю двох осіб – шахрая і жертви. Переважно у погоні за низькою ціною, вигідною пропозицією особа стає жертвою шахрайства.

Нарешті, останньою причиною досліджуваної злочинної поведінки є неповідомлення жертвами шахрайства про кримінальне правопорушення в кіберполіцію, службу підтримки сайтів, на яких здійснювалась покупка, а у разі розголошення даних картки – банк. На наш погляд, жертви досліджуваного шахрайства здебільшого не повідомляють правоохоронні органи про кримінальне правопорушення через те, що: 1) бояться виглядати обманутими в очах інших; 2) вважають завдану шкоду незначною, а тому не

бажають боротись за неї; 3) мають абсолютну зневіру в роботу правоохоронних органів.

Таким чином, узагальнюючи результати проведеного аналізу, зазначимо, що вказані соціально-економічні, організаційно-управлінські й морально-психологічні криміногенні чинники шахрайства у сфері електронної торгівлі діють одночасно і в сукупності, проявляються як на зовнішньому, так і на внутрішньому рівнях, посилюючи кількість і якість кримінальних правопорушень у даній сфері. Отже, завданням держави в особі відповідних органів, установ, організацій та посадових осіб є виявлення й ліквідація безпосередньо цих причин й умов, врахування їх при розробленні заходів запобігання досліджуваному кримінальному правопорушенню.

2.3. Віктимологічний та психологічний аналіз взаємодії шахрая і жертви в електронному комерційному шахрайстві

Для аналізу механізму конкретного кримінального правопорушення необхідно вивчати не тільки особу злочинця, а й жертву злочину. Шахрайство – саме те кримінальне правопорушення, яке дозволяє визначити внесок жертви й визначити результат діяльності «пари» – «жертва-злочинець». Роль жертви в механізмі злочину, а саме шахрайстві, може бути різною: від зовсім нейтральної до максимально провокуючої (характеру поштовху) на вчинення злочину [145, с. 58].

На думку вченого А. Ф. Валуб'єва, у кримінології поняття «механізм злочинів» використовується, але його дефініція, як правило, не надається. Аналіз підручників із кримінології наштовхує на висновок, що механізм злочину в них розуміється як динамічна система, яка визначає зміст злочинної діяльності та містить такі елементи, як обстановку злочину, злочинця, способи його дій, потерпілого та його поведінку. Проте ця система розглядається під кутом зору встановлення причин злочинів і розроблення заходів з їх попередження. У юриспруденції як близький термін використовується

поняття «механізм злочинної поведінки», у якому розглядаються такі елементи поведінки злочинця, як формування злочинного наміру, виникнення мотиву, планування, прийняття рішення щодо вчинення злочину, вибір засобів та ін. [146, с. 17].

Науковці **механізм злочинної поведінки** традиційно розуміють як зв'язок і взаємодію зовнішніх факторів об'єктивної дійсності й внутрішніх, психічних процесів і станів, що детермінують рішення вчинити злочин, направляючих і контролюючих його виконання [147, с. 126]. У наш час розроблена схема механізму злочинної поведінки, яка складається з таких етапів: 1) формування мотивації; 2) прийняття рішення, планування; 3) виконання рішення; 4) посткримінальна поведінка.

До сказаного додаємо, що у структурі системи механізму злочинної поведінки головна роль відводиться мотивації. Ґрунтуючись на досягненнях психологічної науки, О. В. Лисодєд зробив висновок, що в кримінології склалися три основні підходи до розуміння **мотивації злочинної поведінки**. По-перше, поняття «мотивація» вживається для характеристики комплексу мотивів, властивих тій чи іншій особі або тій, чи іншій формі поведінки. По-друге, мотивація злочинної поведінки розуміється як процес виникнення й формування мотиву злочину, його оформлення і розвитку, а потім реалізації у фактичних злочинних діях. По-третє, мотивація розглядається як внутрішній стрижень генезису злочинної поведінки в цілому, результуюча взаємодії особистості злочинця з соціальним криміногенним середовищем (мотивація в широкому сенсі) [45, с. 132]. Разом із цим мотив поведінки – це внутрішнє спонукання до дії, бажання, яке визначається потребами, інтересами, почуттями, що виникли й загострилися під впливом зовнішнього середовища й конкретної ситуації. Слідом за мотивом формується мета як передбачуваний та бажаний результат певної діяльності. Таким чином, якщо розглядати мотив (від лат. movere – рухати, штовхати) як внутрішньо усвідомлене спонукання, яке відбиває готовність людини до дії чи вчинку [148, с. 107], то у нашому

випадку шахрай завжди переслідує корисливий мотив. Слід зауважити, що користь – це одержання майнової вигоди, задоволення будь-яких особистих потреб матеріального характеру [149, с. 15]. Водночас корисливий мотив кримінального правопорушення – це внутрішнє спонукання суб'єкта злочину задовольнити особисті потреби матеріального характеру; а корислива мета – це спрямованість діяння суб'єкта злочину на збагачення, одержання майнової вигоди для себе чи для інших [150, с. 180].

Наступний етап, що посідає особливе місце у структурі механізму злочинної поведінки через прогностичну й спонукальну функції, а також суттєво впливає на обрану модель поведінки, є **прийняття рішення про вчинення кримінального правопорушення**. Звісно, що рішення так чи інакше властиве будь-якому акту поведінки людини та передує йому. Як правило, рішення про вчинення кримінального правопорушення необхідно розглядати як процес і результат здійснення інтелектуально-вольового акту, що виражає готовність особи вчинити конкретне правопорушення. Вказаний процес охоплює усвідомлення, виділення, оцінку й порівняння різних об'єктивних і суб'єктивних факторів, які визначають побудову й вибір різних моделей злочинної поведінки з огляду на можливість їх реалізації в конкретній життєвій ситуації та настання можливих наслідків [151, с. 269]. При прийнятті рішення про вчинення кримінального правопорушення відбувається прогнозування можливих наслідків реалізації задуманого, планування поведінки з урахуванням реальної обстановки, власних можливостей та інших обставин, а також вибір необхідних засобів. Розпочинаючи злочинні дії, особа створює її модель у своїй свідомості, розробляє схеми проведення шахрайської операції, вживає організаційних й технічних заходів, спрямованих на забезпечення можливості її практичної реалізації [152, с. 31]. Зазвичай, після того, як в особи під впливом ситуації та наявних потреб, інтересів, почуттів виникла установка на певну поведінку, настає деяка пауза, людина не діє відразу, а співвідносить її з існуючими моральними, правовими

та іншими нормами, з громадською позицією, з думкою близьких осіб, враховує об'єктивні фактори, у тому числі стан зовнішнього соціального контролю, практику виявлення, припинення кримінальних правопорушень і покарання винних. При цьому зважує всі можливі вигоди й втрати. На цій стадії істотного значення набувають характеристики свідомості особистості, а також осіб і груп, у контакті з якими перебуває особа або на які вона орієнтується. Отже, на стадії прийняття рішення шахрай ще раз співвідносить можливі наслідки свого майбутнього діяння з встановленими в суспільстві нормами поведінки, поглядами й думками. Якщо особа не відмовляється від рішення порушити кримінально-правові заборони, вона обирає ті засоби досягнення мети, які у відповідній обстановці видаються їй найбільш підходящими, при цьому враховує свої власні можливості, можливості співучасників, якщо такі є.

Далі процес вчинення кримінального правопорушення як елемент механізму злочинної поведінки передбачає **реалізацію прийнятого рішення**. У такий спосіб діяння особи зовні набуває юридичного значення (включає всі стадії вчинення кримінального правопорушення й форми співучасті).

Зауважимо, що на поведінку особи при виконанні прийнятого рішення про вчинення кримінального правопорушення вирішальний вплив може мати конкретна життєва ситуація (час, місце, спосіб та ін.). Оцінивши її, особа у змозі змінити план дій, відкласти вчинення кримінального правопорушення або ж відмовитися від його продовження тощо. У цілому, соціальна поведінка особи формується в органічному зв'язку із соціальною дійсністю і залежить від конкретної обстановки, яка склалася в певний момент. Таким чином, лінія поведінки особи може повернути у будь-який бік. З цього приводу О. М. Бандурка стверджує, що не слід гіперболізувати й зменшувати значення об'єктивних умов, які визначають людську поведінку, адже вони перебувають у постійній взаємодії з особистісними властивостями, світоглядом, інтересами індивіда. В основі злочинної поведінки, точніше кажучи, у її причинній

площині, лежить не лише ситуація, а й негативні психологічні деформації, що набули форми суспільно небезпечної настанови особистості. Так, зовнішні фактори діють опосередковано, через риси характеру, вольові й емоційні якості, ціннісно-нормативні характеристики свідомості, мотиваційну сферу і сферу потреб. Умовою переходу зовнішніх факторів у внутрішні є різноманітні форми діяльності людини, кожна з яких відбивається на внутрішньому світі людини [153, с. 115–116]. У цілому найбільш простим варіантом вчинення кримінального правопорушення як елементу механізму злочинної поведінки є фактичне виконання діяння, що призводить до одного чи декількох наслідків; більш складним, коли кримінальне правопорушення включає декілька діянь, які призвели до одного або більше наслідків, ряд діянь, об'єднаних єдиним злочинним умислом. Більш того, процес вчинення злочину може набути форми тривалого злочину.

Нарешті, на етапі пост кримінальної поведінки злочинець аналізує те, що сталося, які настали наслідки, приховує сліди злочину, розпоряджається майном, придбаним злочинним шляхом, вживає заходів для легалізації (відмивання) такого майна, а також вчиняє дії з метою уникнення кримінальної відповідальності (вдається до погроз, усунення свідків, підкупу співробітників правоохоронних, контролюючих органів тощо).

Сутність вищевикладеного зводиться до того, що злочинна поведінка шахрая має такі особливості: 1) стійкість злочинного мотиву й мотивації; 2) пролонгування прийнятого рішення; 3) стійкі установки на вчинення кримінального правопорушення; 4) створення злочинцем ситуації, яка сприяє вчиненню кримінального правопорушення; 5) переростання вчинення одного кримінального правопорушення в професійну злочинну діяльність [154, с. 126–127].

Додаймо, що відповідно до характеру і змісту віктимологічні детермінанти у суб'єктивній формі зумовлені мотивацією віктимологічної поведінки жертв шахрайства і взаємодією із зовнішніми умовами. У

формально-логічному значенні жертви шахрайства може йтися не стільки про об’єктивно-суб’єктивну характеристику соціального зв’язку, скільки про зв’язок детермінації, коли кримінальне правопорушення об’єктивно виникає через процес віктимізації жертви, тобто жертва усвідомлює свій специфічний соціально-правовий статус, завдяки якому щодо неї вчинено діяння. Зрозуміло, що основою моделювання механізму злочинної поведінки є взаємодія злочинця і жертви на матеріальному, енергетичному та інформаційному рівні [155, с. 119].

У цьому контексті кримінологи дотримуються позиції, згідно з якою кожна жертва наділена певним набором вразливостей, що привертають увагу злочинця. Така властивість людини у кримінології називається віктимністю. Так, професори В. В. Голіна та Б. М. Головкін розглядають **віктимність** як уразливість членів суспільства перед злочинними посяганнями за певних обставин; як понижену здатність розпізнавати кримінальні загрози в конкретних умовах простору і часу і захищатися від них [156, с. 39].

Отже, аналізуючи віктимність жертви, взаємозв’язок жертви та шахрая, першочергово звертаємо увагу на спосіб вчинення шахрайства, що полягає у заволодінні майном або придбанні права на майно жертви, яка перебуває в омані, викликаній діями шахрая, і добровільно передає йому своє майно. Через обман та/або зловживання довірою у момент вчинення шахрайства жертва не розуміє того, що відбувається, або помиляється відносно реальної картини, дійсного значення і намірів злочинця. Як правило, розуміння події приходить після вчинення кримінального правопорушення.

Частково взаємодію шахрая і жертви описала О. В. Кравченко. На думку вченої, характерними рисами такої взаємодії є: 1) широке використання злочинцями психологічних методів впливу на жертву; 2) не усвідомлення жертвою справжньої мети злочинця; 3) добровільна передача жертвою майна або права на майно злочинцеві; 4) використання злочинцями так званих «підставних» людей, які «випадково» опиняються на місці вчинення

кримінального правопорушення; 5) не однозначне ставлення суспільства до шахраїв, які нібито «покарали» людину, яка хотіла «на халяву» отримати певну вигоду [157, с. 6].

Зауважимо, що в цілому взаємовідносини жертви й злочинця виникають внаслідок кримінального конфлікту, який мав місце між ними. До вчинення кримінального правопорушення стосунки, що були між ними, можна віднести до звичайних взаємовідносин, але кримінальний конфлікт, до якого призвели ці стосунки, свідчить про їх відхилення від норми, тобто девіацію у процесі їх розвитку і протікання [158, с. 289]. У загальному вигляді взаємодія злочинця і жертви в механізмі вчинення шахрайства може бути представлена наступними елементами, які відтворюють ключові етапи розвитку кримінального правопорушення: 1) вибір жертви, тобто визначення типу жертви (стать, вік, соціальне становище, професія тощо), спосіб вибору жертви, спосіб первинного контакту з жертвою; 2) вибір місця вчинення злочину; 3) розподіл ролей при груповому шахрайстві; 4) «легенда» – вигадана історія чи спеціально інсценована ситуація для жертви правопорушення, яка здається їй правдоподібною, у такий спосіб шахрай впливає на свідомість потерпілого; 5) дії шахрая, безпосередньо направлені на обман потерпілого; 6) засоби обману; 7) спосіб безпосереднього заволодіння чужим майном або придбанням права на нього; 8) дії шахрая на етапі закінчення кримінального правопорушення.

У кримінологічній віктимології існує давня (і обґрунтована) гіпотеза про те, що у кожного злочинця є своя жертва. Це означає, що кожен шахрай має достатнє уявлення про свою потенційну жертву і при її виборі керується не лише зовнішніми характеристиками особи (вік, стать, ознаки хвороби, вартість одягу, наявність авто, прикрас та ін.), а й соціально-психологічними ознаками: інтересами, поглядами, переконаннями. Саме тому вчені виокремили так звані «мішені» маніпулятивного впливу – психічні структури, на які впливає шахрай. До них відносять: 1) матеріальну зацікавленість жертви; 2) споживчі інтереси (придбання товарів, отримання послуг, відновлення здоров’я та ін.); 3)

«благородні» наміри (співчуття, бажання допомогти, щедрість та ін.); 4) особисті почуття (прив'язаність, симпатія, інтимні почуття та ін.); 5) особисті якості жертви (користь, жадібність, навіюваність, довірливість, чесність, самовпевненість та ін.) [159].

Своєю чергою, проведене нами опитування потенційних жертв шахрайства у сфері електронної торгівлі в межах групи питань щодо електронного комерційного шахрайства, крім вирішення інших завдань такого роду досліджень, дозволило з'ясувати низку специфічних, маркерних, привабливих для інтернет-шахрая, типових віктимних рис і характеристик потенційної жертви шахрайства у сфері електронної торгівлі та на підставі їх аналізу зробити висновки.

Переважна частина, а саме **54,7 %,** респондентів вважає, що **довірливість** особи є найбільш привабливою для шахраїв. Спеціалісти в галузі психології та соціології відмічають те, що довіра регулює відносини із навколишнім світом, формує і відтворює соціально-психологічний простір людини. Експерти виокремлюють три основні рівні довіри: когнітивний, емоційний і поведінковий. Когнітивний складається з уявлень про себе, про інших учасників довірливих стосунків, а також очікувань, пов'язаних із його поведінкою; емоційний характеризується емоційними оцінками сторін, які взаємодіють, й оцінками процесу такої взаємодії; і нарешті, поведінковий, який включає готовність до певних дій щодо другого учасника, тих умов, які склалися. У цілому існує довіра до себе, до світу та до інших [160, с. 129]. Як правило, можна виокремити два типи довіряючих осіб: ті, хто довіряють слабо; та ті, хто схильні проявляти високий рівень довіри. Перші не довіряють стороннім людям доти, доки у них відсутні чіткі докази того, що довіряти можна, на відміну від інших, яких легко обманути, оскільки вони, певною мірою, готові вірити незнайомцям за відсутності чіткої інформації, доказів того, що їм довіряти не можна [161, с. 32].

На таку рису, як **«віра у щасливий випадок, везіння, фарт»**, вказали **13,2 %** респондентів; і це, безсумнівно, говорить про недостатню критичність жертв електронного комерційного шахрайства.

Досить високий відсоток (**12,2 %**) опитаних респондентів указали, що саме через **неуважність** особа стає жертвою шахраїв. У психології увага – це пізнавальний психічний процес, який полягає у спрямованості та зосередженості психічної діяльності на певних об'єктах і явищах, що мають сталу або ситуативну значущість для особистості. Якщо увага стає настільки притаманною людині, що характеризує її тривалі психічні стани, вона розглядається як характерна риса особистості, тобто уважність [162, с. 138]. Безспірно, що як уважність, так і неуважність позначаються на всіх сторонах життя особи. З одного боку, уважність виступає важливою умовою чуттєвого й раціонального зображення дійсності, логічного ходу думки та її позитивних результатів, а з іншого – неуважність завжди пов'язана з невмінням довільно регулювати увагу, що негативно позначається на розумовій діяльності особи, порушуючи послідовність, доказовість, несуперечливість суджень, викликаючи емоційне відволікання думки [163, с. 136], тобто неуважна особа не замислюється над причинами й наслідками своєї поведінки, не помічає зміни обставин і деталей ситуації, не враховує психологічного стану оточення й свого особисто, вона діє імпульсивно, механічно, необачливо й безтурботно.

Вказівку на таку рису, як **жадібність**, надали **11,5 %** опитаних. Характерно, що ставлення до грошей – важливий компонент економічної свідомості людини. Зарубіжні вчені, які досліджують психологію грошей, з'ясували, що ставлення людей до грошей неоднозначне, мотивуючи це тим, що гроші, з одного боку, – це показник успіху і благополуччя людини, а з іншого – соціально-засуджуваний фактор, який частіше приносить зло, ніж добро. Одним із таких негативних проявів впливу фінансів на особу виступає жадібність. Цікаво, що семантичне значення слова «жадібність» у багатьох мовах подібне або схоже: у мовах слов'янських груп воно пов'язане зі словом

жадати – бажати, бути нескромним у своїх бажаннях; в англійській та родинних германських мовах – походять від græd або grædig, що означає жадібний або нетерплячий [164, с. 467]. Зазвичай, жадібність проявлятися як користолюбство, надмірне прагнення, бажання, хотіння або ненаситність когось або чогось. Говорячи про жадібність, наголошуємо, що це щось більше ніж надмірне бажання великої кількості грошей або багатства (жадібність до грошей), люди можуть бути жадібними до їжі, влади або чогось іншого. Крім того, серед психологів панує думка, відповідно до якої жадібність – це не лише якісна характеристика особистості, а й соціально-культурний феномен. Для прикладу, психолог А. Маслоу припустив, що здорові люди мають ряд потреб, які розташовуються у вигляді ієрархічної структури. Така «ієрархія потреб» представлена у вигляді п'ятирівневої піраміди, з базовими потребами внизу і більш високими – вгорі. Науковець припускає, що проблема жадібності полягає в тому, що вона зупиняє людину на нижніх рівнях піраміди, тим самим заважає піднятися на рівень самореалізації [165]. Можемо підсумувати, що у жадібних людей ніколи не буває достатньо грошей, вони живуть у страху втратити джерело доходу. Так само як алкоголізм, наркоманія, ігроманія, жадібність – це залежність, заснована на неправильній вірі особи, зазвичай, закладеній ще в дитинстві, що в житті важливими є кількість грошей, статус або влада, що може досягти крайньої межі, несучи загрозу як самій особі, так і її оточенню.

Рису «**схильність до азарту**» відмітили **2,8 %** респондентів. Слово «азарт» не має однозначного розуміння. У перекладі з італійської «azzard» означає ризик, з французької «hazard» – випадок, випадковість; з арабської «az zahr» – гра в кості. Тоді як з точки зору психології, азарт – одна з найбільш неоднорідних людських емоцій, пов'язана з передчуттям успіху. Аналізуючи залежність від азартних ігор, учений В. М. Великий розглядає азарт як: 1) сильне натхнення, піднесення, запал, захоплення; 2) запальність, прагнення до виграшу за будь-яку ціну. На його думку, перший варіант не пов'язаний з

негативною оцінкою, оскільки може характеризувати поведінку творчої цілеспрямованої особистості, яка докладає максимум зусиль задля досягнення результату й отримує задоволення від процесу його досягнення. На відмінну від другого варіанта, що характеризує метушливі, легковажні, необдумані й невиправдані дії, у яких позитивний результат залежність не стільки від майстерності, скільки від везіння [166, с. 51–52]. До того ж учені пояснюють, що природа азарту людини пов'язана з так званим «гормоном щастя», дофаміном, – активною хімічною речовиною, яка виробляється головним мозком людини. Природні викиди цього гормону під час процесів, які приносять нам задоволення, допомагають мозку закріпити важливі дії та події й формують прив'язаність. З огляду на це люди міняють свою поведінку під час сильного захоплення якимось процесом. У цілому азарт, як і пристрасть, змушує людей діяти та ще більше втягує в певні процеси.

Крім того, на думку **2,1 %** респондентів, основною причиною того, що особа стає жертвою шахрайства, є **безвідповідальність**. Узагалі, у суспільстві безвідповідальність звикли розуміти як негативну морально-духовну якість особи, що проявляється в небажанні чи нездатності нести відповідальність за свої слова, вчинки й діяльність. Безвідповідальна особа не має конкретної мети, вважає за краще плисти за течією, не виконує домовленостей, зазвичай дає завідомо неправдиві обіцянки, через силу приймає важливі рішення, якщо береться за справу, то виконує її неякісно, абстрагується від наслідків своєї поведінки, завжди до останнього заперечує свою провину, перекладає відповідальність на інших, а у надзвичайних ситуаціях панікує, не може взяти себе в руки. До типових варіантів безвідповідальності можна віднести звички покладатися на «авось», відкладати все на потім, не думати про майбутнє. Останні дослідження соціологів продемонстрували, що мозок активних користувачів соціальних мереж, завзятих онлайн-гравців, тобто тих людей, для яких віртуальна реальність стає такою ж достовірної, як і дійсність, входить у стан функціональної регресії. Це означає, що мозок дорослої

людини починає працювати дитячими схемами, ніби опускаючись на кілька сходинок вниз, що створює фізіологічні передумови для формування безвідповідального підходу до життя [167].

До того ж цікавим є те, що лише **1,7 %** респондентів вважають, що шахрая привертають особи, схильні до **навіювання**. Основою для такого безпосереднього психічного впливу на свідомість людини, як навіювання є довіра. У психології навіювання – це цілеспрямований, переважно емоційно-вольовий вплив однієї людини на іншу чи групу людей, що здійснюється у вербальній або невербальній формах. До речі, існує усталена наукова думка, що навіювання – це переважно емоційно-вольовий вплив, що викликає певний психічний стан людини, який не підлягає логіці міркувань. Інакше кажучи, психіатр розглядав навіювання як метод психічного впливу на особистість, розрахований на придушення волі людини та підпорядкування вимогам особи, яка його здійснює [168, с. 269]. У наші часи І. О. Гарбан під навіюванням пропонує розуміти прямий, заздалегідь спланований, іноді імпровізований психічний вплив, здійснюваний у гіпнотичному стані з метою зміни психічного й емоційного стану адресату. Учений таке навіювання називає «материнським» видом психічного впливу, що характеризується м'яким, заспокійливим, «тонізуючим», головним чином, доброзичливим і кооперативним характером, здійснюється м'яко, без насилля, оминаючи свідомість особи [169, с. 48]. Здебільшого навіювання є компонентом звичайного людського спілкування, але одночасно може виступити спеціально організованим видом комунікації, що передбачає некритичне сприйняття інформації.

Своєю чергою, кримінологи виявили, що під час вчинення кримінального правопорушення шахраї застосовують маніпулятивні прийоми. Кримінальне маніпулювання здійснюється в комунікативному процесі під час взаємодії злочинця і жертви з використанням комплексу методів і прийомів, у тому числі сучасних психотехнологій. Так, А. С. Булатов стверджує, що під

час вчинення традиційного шахрайства злочинець може: 1) підлаштовуватися до стану потенційної жертви; 2) установлювати з нею психологічний контакт; 3) застосовувати навички самопрезентації; 4) створювати хибний імідж; 5) експлуатувати психічні та/або психологічні автоматизми; 6) маніпулювати змістом, формою та темпом надання інформації; 7) експлуатувати груповий тиск на особистість; 8) створювати штучний дефіцит часу під час прийняття рішення потерпілим [170, с. 207]. У той час як Л. М. Прудка, досліджуючи психологічні особливості шахрайства в мережі Інтернеті, робить висновок, що основними прийомами злочинного маніпулювання свідомістю й поведінкою жертви інтернет-шахрая, у тому числі й у сфері електронної торгівлі, є: 1) маніпулювання змістом і формою надання інформації; 2) створення штучного дефіциту часу у прийнятті рішення (вимагання сплатити неіснуючу послугу або товар у найкоротший строк) тощо [171, с. 31]. Проводячи паралель між кримінальним маніпулюванням і критеріями визначення маніпулювання в цілому, можемо відмітити, що злочинець-маніпулятор (або група таких) під час вчинення шахрайства у сфері електронної торгівлі ставиться до жертви виключно як до засобу досягнення власних цілей, намагається отримати односторонній виграш – заволодіти майном. При цьому успішність шахрайства залежить не лише від уміння злочинця приховати спрямованість впливу, його кінцеву мету, а й від деяких психофізіологічних факторів, що сприяють зниженню рівня свідомого контролю особи, підвищують навіюваність й імпульсивність, серед них: стан втоми або голоду, ізоляція від зовнішніх контактів, ліміт часу для прийняття рішення, спеціально підібраний музичний фон.

Даним щодо навіюваності кореспондують вказівки на **самовпевненість**. Про останню респонденти зазначають теж вкрай неохоче (**менш** як **2 %**). У юриспруденції злочинна самовпевненість – це вид злочинної необережності, коли особа передбачає можливість настання суспільно небезпечних наслідків своєї дії або бездіяльності, але легковажно розраховує на їх відвернення.

Психологи ж самовпевненість розглядають як перебільшену впевненість особи у власних силах, переконаність у своїй досконалості й відсутності помилок. За даними останніх психологічних досліджень, причиною невдач переважно виступає зайва самовпевненість, оскільки особа, якій вона притаманна, розглядає свої сили й реальні перспективи спотворено, з ідеальної точки зору, як наслідок, це заважає досягти успіху. Такі люди не визнають помилок, а зіткнувшись з невдачами, списують їх на обставини, спотворено сприймають реальне співвідношення проблем з їх внутрішніми силами, що порушує адекватність мислення [172].

Таким чином, аналіз основних показників дозволяє зробити висновки щодо узагальненого «портрету» жертви шахрайства у сфері електронної торгівлі.

1. Особи, які обрали варіант відповіді «довірливість» і «віра в щасливий випадок, везіння, фарт», скоріш за все, виправдовують себе.

2. Більш ніж половина респондентів (а саме, 67,9 %) ставали жертвами шахрайства або ж мали досвід шахрайства, однак належним чином не проаналізували свою поведінку, відповідну життєву ситуацію і висновків щодо цього не зробили.

3. Вказівки на жадібність і неуважність (23,7 %) окреслюють велику позитивну категорію жертв, здатних мислити критично і робити логічні висновки. У цьому контексті зауважимо, що жадібність знижує критичне мислення, а неуважність стосується способів шахрайства (неуважну особу легко обманути).

4. Варіанти «азарт», «безвідповідальність» і «самовпевненість» не знайшли підтримки (6,6 %) без розумних на те причин. Хоча, з точки зору кримінології, ці результати цілком пояснювані та інформативні. Такі риси характеру відтворюють справжні мотиви поведінки жертви, які далеко не завжди є благородними, і лише ця невелика, ледь 7-відсоткова, категорія жертв демонструє вміння критично оцінювати свою поведінку і критично ставитись до себе.

5. Також результати дослідження вказують на вірогідність гіпотези, що ймовірність стати жертвою шахрайства у сфері електронної торгівлі вища у жадібних і довірливих осіб, у яких відсутнє або погано розвинене критичне мислення та яким не відомі сучасні способи шахрайства. Поряд із цим високою віктимністю характеризуються особи, які мають гарну освіту (більшість з них вищу), ведуть активний спосіб життя, пізнають нові види діяльності, однак це – азартні самовпевнені люди, які люблять ризик, вірять у щасливий випадок.

Зі сказаного раніше випливає, що жертвам досліджуваного шахрайства притаманні специфічні відмінні риси, які включають не скільки соціально-демографічні, а переважно морально-психологічні групові характеристики, наведені у нашому дослідженні.

Отже, можемо стверджувати, що знання як загальних особливостей психіки людини, так і пізнання групових особливостей віктимних осіб дозволяють шахраю вибудовувати взаємодію з жертвою під час вчинення кримінального правопорушення.

На думку К. Л. Попова, діапазон взаємодії «злочинець-жертва» при шахрайстві різноманітний: від хвилинних контактів без встановлення будь-яких стосунків до багаторічних тісних взаємовідносин між майбутнім шахраєм і жертвою. Учений контакт між шахраєм і жертвою класифікує на: тілесний (зоровий, слуховий); емоційний (співпереживання); знаковий (жести, міміка); операціональний (розуміння дій іншого та сигналізування про це); предметний (вірне тлумачення взаємних повідомлень); особистісний (розуміння індивідуальних смислів іншої людини); духовний (об’єднання на основі високих смислів та цінностей) [173, с. 209].

У свою чергу, вважаємо, що **контакт між шахраєм і жертвою шахрайства у сфері електронної торгівлі є дистанційним**. Злочинець позбувся аудіовізуального портрета жертви. Образно висловлюючись, шахрай закидає не «гачок», а велику «рибальську сітку», розраховуючи «піймати»

некритичних, імпульсивних осіб із низькою інформативною і загальною грамотністю, незалежно від віку і рівня освіти.

Отже, взаємодія злочинця і жертви шахрайства у сфері електронної торгівлі зумовлюється і коригується такими обставинами, як: відділений, дистанційний, вкрай опосередкований контакт між шахраєм і жертвою; неможливість скласти аудіовізуальний портрет жертви (як при «класичному» шахрайстві); необхідність визначення цільової «аудиторії», яка в умовах масового використання цифрових технологій значно розширилася.

Висновки до розділу 2

Кримінологічний аналіз стану і динаміки вчинення шахрайств у сфері електронної торгівлі було зроблено на основі: 1) обчислення кількості зареєстрованих кримінальних правопорушень, ознаки складу яких містять у собі ознаки шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки у сфері електронної торгівлі; 2) вивчення обвинувальних вироків щодо осіб, які були засуджені за ч. 3 ст. 190 КК України; 3) визначення способу вчинення кримінального правопорушення й з’ясування інших особливостей вчинення електронного комерційного шахрайства.

Внаслідок дослідження було встановлено регулярні випадки шахрайства у сфері електронної торгівлі. Проте рівень притягнення винних осіб до кримінальної відповідальності є низьким. Виявлено, що вчинення електронного комерційного шахрайства здійснюється шляхом отримання повної передплати (у 64 % випадків), часткової передплати (у 23,3 % випадків), одночасного поєднання цих двох способів (у 4,9 % випадків), підміни товару (у 12 % випадків), фішингу (у 3 % випадків), крадіжки й використання персональних банківських даних (у 3 % випадків), вішингу (у 0,6 % випадків).

Констатовано, що спостерігається тенденція до вчинення електронного комерційного шахрайства на таких основних майданчиках (площадки), як: aukro.ua, ВКонтакті, Однокласники, Olx.ua, Facebook, Instagram. Встановлено категорії товарів і послуг електронної комерції, якими псевдопродавці (шахраї) «приваблюють» жертв. Серед них: побутова техніка, електроніка (34 %), товари загального вжитку (24 %), одяг і взуття (27 %), транспортні засоби й запчастини до них (10 %), оренда нерухомості (4 %), косметика і парфумерія (1 %) тощо.

При вивченні причин й умов шахрайства у сфері електронної торгівлі встановлено, що найбільший вплив на рівень шахрайства у сфері електронної торгівлі мають: стрімкий перехід торгівлі з офлайн-режиму в онлайн, викликаний коронавірусною кризою, упровадження нових технологій, недосконаліть законодавства у сфері електронної торгівлі, недосконаліть нормативно-правової бази у сфері кібербезпеки, перехід від реального спілкування до віртуального, переважаючий емоційний інтелект людей, ігровий характер поведінки. Дослідження причин й умов вчинення крадіжок у сфері електронної торгівлі показало доцільність їх поєднання у три основні групи чинників: соціально-економічні; організаційно-управлінські; морально-психологічні.

Проведення віктимологічного й психологічного аналізу взаємодії шахрая і жертви в електронному комерційному шахрайстві продемонструвало те, що жертва наділена наступним набором уразливостей, які привертають увагу злочинця: довірливість – 54,7 %, віра у щасливий випадок, везіння, «фарт» – 13,2 %, неуважність – 12, 2 %, жадібність – 11,5 %, азарт – 2,8 %, безвідповідальність – 2,1 %, навіюваність – 1,7 %, самовпевненість – 1,7 %.

Доведено, що ймовірність стати жертвою електронного комерційного шахрайства вища в осіб, які характеризуються високим рівнем довіри, у яких відсутнє або погано розвинене критичне мислення та яким не відомі сучасні способи шахрайства; в азартних самовпевнених людей, які люблять ризик,

вірять в щасливий випадок, при цьому мають гарну освіту (більшість з них вищу), ведуть активний спосіб життя, пізнають нові види діяльності.

Зауважено, що контакт між шахраєм і жертвою електронного комерційного шахрайства є дистанційний.

РОЗДІЛ ІІІ
ТЕОРІЯ І ПРАКТИКА ЗАПОБІГАННЯ ШАХРАЙСТВУ У СФЕРІ ЕЛЕКТРОННОЇ ТОРГІВЛІ

3.1. Зарубіжний досвід запобігання електронному комерційному шахрайству та перспективи його застосування у вітчизняній практиці

Результати проведеного нами дослідження, викладені в попередніх підрозділах, вказують на те, що шахрайство у сфері електронної торгівлі – це дуже поширене протиправне діяння, вчинення якого завдає багатомільйонних збитків, вирізняється організованим характером, складністю виявлення і запобігання. Враховуючи це, а також непросту криміногенну ситуацію в електронній торгівлі, необхідно, по-перше, віднайти універсальні механізми ефективного запобігання кримінальним правопорушенням у цій сфері, оскільки це дозволить напрацювати концептуальні заходи державної політики протидії шахрайствам, по-друге, розробити програму (план) дій для правоохоронних органів.

З огляду на сказане, добавимо, що з електронним комерційним шахрайством зіштовхуються правоохоронні органи не тільки в Україні, а й в інших державах із розвиненою електронною комерцією. Однак світовою спільнотою до тепер не було вироблено ефективної моделі протидії цим злочинам.

Нагадаємо, що електронна комерція й електронна торгівля посідають провідне місце в економіці зарубіжних держав, особливо в умовах запровадження соціальної дистанції, карантину та інших обмежувальних

заходів у період пандемії COVID-19. Починаючи з 2019 р. по 2021 р. відбулося значне зростання світової електронної комерції у сегментах B2B і B2C. За даними Forbs, інтернет-магазини США станом на 2020 рік збільшили свої доходи на 68 %, у порівнянні з 2019 р. [174], а кількість інтернет-замовлень у США й Канаді виросла у 2,5 раза [175]. Така тенденція у сегменті B2C простежується серед продажу предметів медичного призначення, предметів першої необхідності, продуктів харчування, електроніки та ін. Згідно з даними дослідження Deloitte, у Данії 65 % дистриб'юторів продуктів харчування повідомили про приріст доходів більш ніж на 10 %, у той час, як продаж предметів розкоші й інтер'єру значно знизився [176]. До того ж цікаво, що криза COVID-19 призвела до підвищення попиту на використання телемедичних послуг. У Китаї медичні онлайн-платформи показали тризначний темп зростання у період з грудня 2019 року по січень 2020 року (до 900 відсотків) [177].

Зауважимо, що кількісні оцінки електронної комерції частіше за все, крім маркетингових агентств, надають міжнародні організації, серед них на особливу увагу заслуговує діяльність ООН. Відповідно до даних 2021 року, які наводяться у доповіді Конференції ООН з торгівлі та розвитку (далі – ЮНКТАД), у 2020 р. онлайн продажі склали п'яту частину всіх роздрібних продажів. За рік цей показник збільшився із 16 до 19 %. Більш того, за даними доповіді ЮНКТАД, лідерами з використання ІКТ у сфері торгівлі є США і Китай, на їх частку припадає 50 % світових гіпер масштабних центрів обробки даних, а також у цих країнах фіксуються найвищі показники впровадження 5G (п'ятого покоління стільникового зв'язку), зосереджено 70 % провідних світових дослідників штучного інтелекту [178].

Зрозуміло, що масштабний розвиток електронної комерції та електронної торгівлі призводить до зростання кількості шахрайств у цій сфері. Говорячи комерційною мовою: попит породжує пропозицію.

Аналізуючи міжнародний досвід запобігання електронному комерційному шахрайству, відмітимо, що в англомовних країнах існує термін ecommerce fraud, який перекладається як шахрайство у сфері електронної торгівлі, або шахрайство з платежем. Відповідно до визначення BigCommerce[16], **ecommerce fraud** – це злочинний обман, що вчиняється під час здійснення комерційної транзакції через мережу Інтернет з метою отримання фінансової або будь-якої іншої особистої вигоди шахрая й негативно впливає на чистий прибуток продавця.

Порівнюючи крадіжки в мережі роздрібної торгівлі з шахрайством у сфері електронної торгівлі, віцепрезидент американської компанії ClearSale, яка надає послуги з виявлення шахрайських угод у сфері електронної комерції, Р. Лоуренко запевняє, що основними причинами, а одночасно й умовами ecommerce fraud є:

1) **легкість**. До появи Інтернету, щоб заволодіти чужим майном, злочинцеві доводилося красти кредитні картки, а лише потім ними можна було оплачувати покупки. Зрозуміло, що це дуже ризикова справа, у порівнянні з тим, що сьогодні шахраї мають можливість придбати вже вкрадені кредитні картки в необмеженій кількості в мережі Інтернет. Як наголосив Р. Лоуренко, у першій половині 2019 року в мережі Інтернет було виставлено на продаж не менше 23 мільйонів вкрадених кредитних карток;
2) **анонімність**. У діджиталізованому суспільстві у шахраїв відпадає необхідність йти до магазину, із кимось говорити або ризикувати потрапити на камери відеоспостереження, вони можуть працювати з будь-якого місця, будь-коли, а головне, непомітно. Усе, що їм потрібно, – комп'ютер і підключення до глобальної мережі. Зазвичай інтернет-шахраї

[16] BigCommerce – це платформа електронної комерції, що входить до списку NASDAQ і надає програмне забезпечення як сервісну послугу роздрібним торговцям. Платформа компанії включає створення інтернет-магазинів, оптимізацію пошукових систем, хостинг, маркетинг і безпеку від малого до великого бізнесу.

не розкривають особистої інформації про себе, вони створюють підроблені облікові записи електронної пошти та/або орендують поштові скриньки, використовують псевдоніми;

3) **ухилення**. Досвідчені злочинці знають, що у США поліціанти не відносять шахрайство у сфері електронної торгівлі до пріоритетних справ, оскільки сума завданої шкоди зазвичай невелика, у порівнянні з іншими видами злочинів. Крім того, таке шахрайство все частіше виходить за межі однієї держави, ускладнюючи роботу поліції з виявлення й переслідування онлайн-злочинців в інших країнах [179].

Нині міжнародна спільнота дуже занепокоєна поширенням і значним підвищенням кількості випадків електронного комерційного шахрайства, оскільки заподіюється шкода не тільки продавцям та/або споживачам, а й економікам держав. Так, за даними звіту FIS Global Payment Risk Mitigation Report 2021, проведеним Worldpay, дев'ять із десяти (89 %) багатоканальних і корпоративних продавців із 11 країн внаслідок шахрайства з платежами втратили частину доходу, із них 38 % продавців повідомили, що їх втрати становлять понад 6 % річних прибутків [180]. Крім того, відповідно до даних LexisNexis Risk Solutions, «ціна» електронного комерційного шахрайства у 2020 р. зросла на 7,3 % у річному обчисленні. За їх підрахунками, один втрачений долар у результаті такого шахрайства «коштує» компаніям близько 3,36 дол. [181]. Водночас останнє дослідження Juniper Research підтверджує, що упродовж 2021 року загальний розмір втрат у сфері електронної комерції внаслідок шахрайства збільшився на 18 % (зріс з 17,5 млрд дол. у 2020 р. до понад 20 млрд дол. у 2021 р.). Дослідження показало, що шахраї орієнтовані на споживачів, відслідковуючи, як серед останніх підвищується інтерес до електронної торгівлі [182]. Для порівняння, загальна кількість транскордонного шахрайства у США у 2020 році склала 33 968 випадків, заявлені збитки сягнули 91,95 млн дол. США, а п'ятьма роками раніше було зареєстровано 14 797 таких заяв (сума збитків становила 40,83 млн дол. США).

Як бачимо, загальний обсяг транскордонного шахрайства в США за 5 років виріс більш ніж у 2 рази. Проте до правоохоронних органів потерпілі звертаються переважно зі скаргами на: 1) обман при покупках в Інтернеті; 2) спотворення інформації про товари; 3) випадки, коли не доставлявся придбаний товар та 4) з проблемами повернення втрачених коштів. Враховуючи наведену статистику, США посіли перше місце серед десяти країн за кількістю поданих скарг до правоохоронних органів на шахрайство у сфері електронної комерції, поряд з Індією, Польщею, Австралією, Великою Британією, Канадою, Туреччиною, Іспанією й Мексикою. Найбільше відповідних скарг надійшло на компанії, зареєстровані в Китаї, Великій Британії, Франції, Іспанії, Канаді, Польщі й Туреччині [183].

Виходячи з наведеного, стає очевидно, що належний захист споживачів – актуальна глобальна проблема у сфері електронної комерції, саме тому її вирішення на світовому рівні було покладено на: 1) Організацію економічного співробітництва та розвитку (далі – ОЕСР) і ЮНКТАД, діяльність яких спрямована на захист прав споживачів із метою формування здорової й конкурентоспроможної міжнародної торгівлі; 2) засновану у 1960 р. Consumer International (CI) – групу організацій-споживачів у більш ніж 100 країнах, які представляють і захищають права споживачів на міжнародних політичних форумах і світовому ринку (налічує близько 250 таких членів); 3) інші провідні міжнародні агенції, діяльність яких спрямована на забезпечення здорової конкуренції в національній і міжнародній торгівлі, у тому числі й електронній, а саме: European Consumer Centres Network (ECC Net), APEC Electric Commerce Steering Group, Ibero-American Forum of Consumer Protection Agencies (FIAGC). Однак, завдання запобігання електронному комерційному шахрайству більш дієво вирішується, на наше переконання, на державному рівні.

Слід врахувати, що у країнах з високорозвиненою електронною комерцією, таких, як США або країни Азії (Китай, Індія, Північна Корея),

особлива увага приділяється захисту (у тому числі запобіганню кримінальним правопорушенням) суб'єктів, які провадять електронну комерційну діяльність, від загроз шахрайства.

На основі узагальнених результатів вибіркового вивчення вироків у кримінальних справах щодо шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки, можемо зробити висновки, що в Україні жертвами електронного комерційного шахрайства в 96 % випадків стають споживачі, а не представники електронного бізнесу. Проте така інформація є неточною. Пояснюємо це тим, що інтернет-магазини, служби доставки та ін., задля зберігання своєї репутації замовчують факти шахрайства. Через це державні органи України не приділяють належної уваги запобіганню електронному комерційному шахрайству, жертвами якого стають бізнес-суб'єкти.

Спираючись на це, вбачається за доцільне вивчити досвід інших країн. Далі розглянемо основі види електронного комерційного шахрайства, жертвами якого стають суб'єкти, які провадять електронну комерційну діяльність (на прикладі США).

1. **Credit card fraud,** або шахрайство з кредитними картками, шахрайство з платежем. Під час такого шахрайства злочинець сплачує покупку товарів або послуг онлайн, використовуючи дані вкраденої кредитної картки. Для цього шахраї спочатку купують дані вкраденої кредитної картки в мережі Інтернет.

2. **Affiliate fraud,** або партнерське шахрайство, метою якого є отримання партнерських комісій шляхом обману або зловживання довірою. Загалом, з метою залучити більше споживачів компанії співпрацюють між собою. Зокрема, компанія А. розміщує на своєму сайті унікальне вебпосилання партнера – компанії Б., яке направляє споживачів на сайт останньої, взамін компанія Б. сплачує партнерові комісію з продажів, зазвичай у відсотках від ціни проданої продукції. У такий спосіб при партнерському шахрайстві дії

злочинця спрямовані на отримання партнерських комісійних або ж на збільшення їх суми.

3. **Chargeback fraud,** або шахрайство зі зворотним платежем. За типовим сценарієм шахрайства зі зворотним платежем, спочатку шахрай здійснює покупку в інтернет-магазині, після отримання товару вижидає певний проміжок часу (від тижня до місяця), зв'язується зі своїм банком і заперечує транзакцію, стверджуючи, що вона була несанкціонованою або шахрайською, сподіваючись, що у продавця не вистачить часу й ресурсів, щоб заперечити його претензії.

4. **Phishing/account takeover**, або фішинг. У цілому для купівлі в інтернет-магазині споживачам необхідно зареєструватися на сайті магазину – створити облікові записи з їх особистою інформацією. Проте шахраї навчилися зламувати такі облікові записи за допомогою різних фішингових схем. Наприклад, злочинці можуть розсилати електронні листи, щоб обманом змусити особу розкрити особисті дані, такі як логін і пароль для входу в обліковий запис електронного банкінгу, увійшовши до якого, змінюють паролі й здійснюють різні несанкціоновані покупки.

5. **Interception fraud,** або шахрайство з перехопленням. Під час цього виду шахрайства злочинці, використовуючи дані викраденої кредитної картки, у тому числі ім'я й адресу власника карти, купують деякий товар в інтернет-магазині й оформлюють його доставку за адресою власника карти, однак все одно «перехоплюють» товар, вчасно змінюючи адресу доставки.

6. **Triangulation fraud,** або тріангуляційне шахрайство. На першому етапі даного виду шахрайства з метою отримання особистої інформації споживачів (ПІБ, домашньої адреси, даних банківських карток) шахраї створюють підроблений сайт інтернет-магазину, як правило, із продажу брендових товарів за низькими цінами. Після цього у справжньому магазині, використовуючи отримані дані покупців, купують саме той товар, який жертва «придбала» у них, і відправляють їй. По завершенні покупки злочинці

використовують вкрадені дані клієнтів за для того, щоб робити онлайн-покупки, але доставку оформлюють уже на себе. Як правило, таке шахрайство важко виявити, оскільки оригінальна покупка з підробленого сайту не викликає жодних підозр у жертви.

Розглянувши основі види електронного комерційного шахрайства, нижче на прикладі країн із найбільш розвиненою електронною торгівлею спробуємо проаналізувати кращі практики запобігання йому. Передусім звернемо увагу на наявність спеціальних законів, які регулюють відносини у цій сфері, і суб'єктів, на яких покладені повноваження із запобігання такому виду шахрайства. Ураховуючи, що за оцінками eMarketer 2021 року, однозначними лідерами з онлайн-продажів у роздрібному сегменті були визначені США і Китай [179], саме на їх прикладі вивчимо зарубіжний досвід запобігання шахрайству у сфері електронної торгівлі.

Так, у США у 1986 р. прийнято спеціальний нормативний акт – Computer Fraud and Abuse Act (Закон про комп'ютерне шахрайство та зловживання), який встановив заборону на доступ до комп'ютера або комп'ютерної мережі стороннім особам без згоди власника [184]. До того ж цим Законом визначена відповідальність за злом і крадіжку даних, знищення й розповсюдження приватної або секретної інформації, заволодіння чужим майном у мережі Інтернет. Більш того, в окремих випадках цей закон дозволяє жертві комерційного шахрайства подавати цивільний позов щодо компенсації шкоди.

Пізніше, а саме у 2003 р., у США був прийнятий Controlling the Assault of Non-Solicited Pornography and Marketing Act, більш відомий як Закон CAN-SPAM [185], що стосується електронних листів, надісланих як комерційна реклама. Відповідно до норм цього Закону: 1) в електронних листах, які містять комерційну рекламу, заборонено використовувати помилкові або ті, що вводять в оману, тематичні заголовки; 2) відправник повинен зазначати в темі листа свою поштову адресу і повідомити одержувача про можливість відмовитися від отримання подібних електронних повідомлень у

майбутньому; 3) заборонено продаж і передачу адрес електронної пошти одержувача. За порушення наведених вимог особа притягується до відповідальності у виді штрафу в розмірі понад 40 000 доларів.

Нарешті, у 2006 р. у США набув чинності Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act (SAFE WEB), більш відомий як Закон про безпеку в Інтернеті. Цей документ регулює правові відносини в мережі Інтернет з метою запобігти спаму, інтернет-шахрайству й обману в мережі [186]. На відміну від інших законодавчих актів, які були зосереджені на боротьбі з кібершахрайством на національному рівні, норми Закону SAFE WEB спрямовані на запобігання й боротьбу з транснаціональним шахрайством. Принагідно додати, що в Законі міститься чіткий перелік заходів захисту інтернет-користувачів від спаму та інших інтернет-атак. Для досягнення цієї мети розширено повноваження Федеральної торговельної комісії (Federal Trade Commission) у сфері боротьби з міжнародним комп'ютерним шахрайством, дозволено передавати конфіденційну інформацію закордонним правоохоронним органам. Це дає комісії змогу активно співпрацювати з іноземними колегами, контролювати міжнародну незаконну діяльність й залучати інші держави до взаємного обміну інформацією.

Перейдемо до іншого моменту. Так, основними суб'єктами, на яких покладені повноваження з запобігання eccomerce fraud, у США є Федеративне бюро, ФБР (Federal Bureau of Investigation, FBI) і Секретна служба (United States Secret Service, USSS).

Як відомо, ФБР – це провідне федеральне агентство з розслідування кібератак та інших злочинних вторгнень. На офіційному сайті ФБР зазначено, що основна мета установи полягає в тому, щоб змінити поведінку злочинців (тобто запобігти кіберзлочинам) та держав, які сподіваються зламати інтернет-мережі США, заволодіти майном або інтелектуальною власністю й поставити під загрозу іншу інфраструктуру, не наражаючи себе на ризик. Як правило, у

своїй роботі ФБР дотримується командного підходу, налагоджуючи постійну співпрацю з федеральними органами, іноземними партнерами й приватним сектором (підприємцями, науковцями), об'єднуючи й спрямовуючи всі зусилля на запобігання електронному комерційному шахрайстві. Слід вказати, що у 2008 р. у межах установи створено Національну об'єднану оперативну групу з розслідування кіберзагроз (National Cyber Investigative Joint Task Force, NCIJTF), до складу якої входить понад 30 партнерських агенцій правоохоронних органів, розвідувальної спільноти й Міністерства оборони. Крім того, у разі необхідності ФБР може створювати спеціально навчені кібергрупи: Групу швидкого реагування (Cyber Action Team), Центр скарг на інтернет-злочини (ІСЗ). Важливо, що, маючи кіберпомічників – юридичних аташе по всьому світові, ФБР тісно співпрацює з міжнародними партнерами [187].

Що стосується Секретної служби США, то її головною метою є захист фінансової інфраструктури країни, створення й підтримка таких умов, за яких американський народ зможе безпечно проводити фінансові операції. Водночас місія служби полягає в розслідуванні складних фінансових кримінальних правопорушень у кіберпросторі. Необхідно додати, що декілька років тому для покращення роботи Секретної служби була створена Цільова група з кібершахрайства, яка виступає основним центром з розслідування шахрайства в мережі Інтернет, співпрацюючи з іншими правоохоронними органами, прокуратурою, приватним сектором і науковими колами. Стратегічна робота групи спрямована на запобігання, виявлення, розслідування кримінальних правопорушень і зменшення заподіяної ними шкоди [188].

Вивчивши досвід запобігання шахрайству у сфері електронної торгівлі в Китаї, зауважимо, що в державі Закон «Про електронну торгівлю» набув чинності 1 січня 2019 р., а його розробка тривала майже 6 років. Згаданий Закон містить положення не лише про електронну торгівлю й захист прав споживачів, а й про заходи боротьби з порушенням прав інтелектуальної

власності й запобігання шахрайству в цій сфері. У цілому дія Закону поширюється на: 1) платформи електронної торгівлі (такі, як TaoBao, Alibaba та ін.); 2) постачальників (юридичних і фізичних осіб), які ведуть комерційну діяльність на таких платформах; 3) фізичних і юридичних осіб, некомерційні організації, які здійснюють продаж товарів через Інтернет або іншу інформаційну мережу. Крім того, Закон містить чіткий перелік інструментів, використання яких забезпечує прозорість і підзвітність суб'єктів електронної торгівлі, а також встановлює відповідальність за порушення його норм. Відповідно до приписів Закону, всі постачальники повинні: 1) пройти реєстрацію для ведення електронної комерційної діяльності (ст. 10); 2) платити податки; 3) отримати необхідні адміністративні ліцензії в тих випадках, коли цього вимагає закон (ст. 11–12); 4) публікувати на домашній сторінці сайту свої комерційні й адміністративні ліцензії, а також іншу інформацію, що стосується їх комерційної діяльності; 5) забезпечувати повноту, конфіденційність і доступність інформації, яка була отримана під час роботи; 6) піклуватися про якість продуктів; 7) повідомити у разі виявлення будь-якого порушення відповідні органи [189].

Разом із вказаним актом у Китаї важливу роль у запобіганні електронному комерційному шахрайству відведено Закону «Про кібербезпеку» (CSL) від 1 червня 2017 р., основною метою прийняття якого було створення окремого суворо контрольованого незалежного кіберпростору і захист електронного бізнесу. Цей Закон зобов'язує суб'єктів електронної комерційної діяльності розробити правила внутрішнього управління у сфері кібербезпеки, вживати необхідних технічних заходів для запобігання комп'ютерним вірусам, атакам і вторгненням, а також іншим діям, що загрожують кібербезпеці, вести моніторинг інцидентів кібербезпеки, вживаючи таких заходів, як: категоризація даних, резервне копіювання, шифрування важливих даних.

Також суворі вимоги до ведення електронної комерційної діяльності містять китайські національні стандарти. Серед них варто згадати багаторівневу систему захисту кібербезпеки 2.0 (MLPS 2.0), основним завданням якої в кіберпросторі є запобігання різному роду втручанням, пошкодженням, несанкціонованому доступу, розголошенню та/або крадіжці електронних даних. Завдяки прийняттю цього стандарту китайські компанії почали впроваджувати надійні й безпечні IT-системи з метою зменшення кількості інцидентів порушення правил безпеки й уникнення їх розслідувань [190].

Узагальнюючи, можна сказати, що в Китаї кіберзлочини, яким приділяється все більше уваги через стрімкий розвиток електронної комерції, підпадають під дію низки нормативних актів. Основними органами, які забезпечують формування й реалізують державну політику у сфері електронної комерції, є Міністерство громадської безпеки КНР, Міністерство промисловості та інформаційних технологій КНР та Інтернет-спільнота КНР. Боротьбу з кримінальними правопорушеннями ведуть поліція КНР і Cyber Security and Technology Crime Bureau (CSTCB), остання розслідує кіберзлочини, здійснює комп'ютерну криміналістичну експертизу, вживає заходів із запобігання кіберзлочинам, встановлює тісні зв'язки з місцевими й міжнародними правоохоронними органами у боротьбі з транскордонними кіберзлочинами [191].

У цілому в зарубіжних країнах склалися усталені правила захисту суб'єктів, які ведуть електронну комерційну діяльність, від різних видів шахрайств, дотримання яких сприяє не лише розпізнанню, а й вжиттю превентивних заходів зі зниження ризиків шахрайства у сфері електронної торгівлі.

Отже, розглянемо кілька інструментів виявлення й запобігання електронному комерційному шахрайству.

1. **Регулярний аудит безпеки сайту** щодо: 1) оновлення програм; 2) актуальності й дієвості роботи сертифіката SSL; 3) дотримання стандарту

безпеки даних індустрії платіжних карток PCI-DSS; 4) наявності резервної копії сайту; 5) надійності паролів облікових записів адміністраторів, панелей керування хостингом, бази даних та доступу по FTP; 6) сканування вебсайту на наявність шкідливих програм; 7) шифрування зв'язку між магазином, покупцями, постачальниками та ін.

2. **Дотримання стандарту PCI DSS**. Інтернет-магазин, який отримує оплату товару шляхом перерахування грошового переказу на картковий рахунок, повинен дотримуватися вимог стандарту PCI DSS. Відповідно до визначення Вільної енциклопедії Вікіпедія, Payment Card Industry Data Security Standard (PCI DSS) – це стандарт 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 і Discover. У цілому цей стандарт складається з 12 деталізованих вимог до забезпечення безпеки даних власників платіжних карток, які передаються, зберігаються й обробляються в інформаційних інфраструктурах організацій [192].

3. **Регулярна перевірка сайту на підозрілу активність.** З метою запобігання шахрайству у сфері електронної торгівлі у зарубіжних країнах власники онлайн-магазинів наймають співробітників, до обов'язків яких належить відстежування підозрілої активності сайту.

4. **Використання служби перевірки адрес (AVS)** - стандарту, який застосовується для зіставлення платіжної інформації із записом до платіжної інформації в точці продажу в дебетових і кредитних картках та допомагає зупинити шахрайство й повернути викрадені кошти. Зазвичай автентифікація AVS використовується як частина багатошарової системи захисту від шахрайства, щоб гарантувати затвердження дійсних транзакцій і відхилення тих, які вважаються підозрілими [193].

5. Послугування **CVV2, CVC2-кодами** – захисними кодами платіжних карток, закодованих у магнітній смузі на їх зворотному боці. Вони потрібні

для того, щоб банк при оплаті товарів та/або послуг карткою міг ідентифікувати клієнта.

6. **Застосування безпечного протоколу передачі гіпертексту (HTTPS)**. Центр Google надав роз'яснення, що Hypertext Transport Protocol Secure (далі HTTPS) – це протокол, який забезпечує цілісність і конфіденційність даних при їх передачі між сайтом і пристроєм користувача. Таким чином, з метою запобігання електронному комерційному шахрайству всім розробникам сайтів рекомендується послуговуватися протоколом HTTPS. До того ж на сайтах, які використовують HTTPS, безпека інформації забезпечується ще й за допомогою протоколу Transport Layer Security (TLS), який передбачає три основні рівні захисту: 1) шифрування переданих даних із метою уникнення їх витоку; 2) забезпечення цілісності даних (будь-яка зміна або спотворення даних, що передаються, фіксуються незалежно від того, було її зроблено навмисно чи ні); 3) аутентифікації користувачів [194].

7. **Зберігання обмеженої кількості інформації**. Один зі способів захистити інтернет-магазин від витоку даних чи злому – зберігати якомога менше даних про клієнтів, адже хакери не можуть вкрасти те, чого немає. Тому рекомендується збирати та зберігати лише ті дані, які необхідні для кінцевої оплати й відправлення товару.

8. **Встановлення обмежень** на кількість покупок та їх загальну вартість, які онлайн-магазин приймає з одного облікового запису протягом одного робочого дня. Це мінімізує ризики у разі шахрайства.

9. **Перевірка IP-адрес**. Кожне замовлення в інтернет-магазині надходить з унікальної загальнодоступної IP-адреси (рядок чисел, розділених крапками, який може ідентифікувати комп'ютер). За IP-адресою можна визначити місто чи регіон, де споживач здійснює покупку. Тож рекомендується цю IP-адресу перевіряти на відповідність адресі кредитної картки споживача.

10. **Використання спеціальних програм для боротьби з шахрайством**. Як правило, коли справа доходить до виявлення і запобігання шахрайству у сфері електронної торгівлі, існує безліч програмних рішень, що відповідають різним потребам і бюджетам. Прості програми боротьби з шахрайством зазвичай інтегровані в платформи електронної комерції або онлайн-кошики. Ці інструменти застосовують різні алгоритми виявлення шахрайських транзакцій, найбільш відомі – перевірки геолокацій IP-адрес, адрес електронної пошти, відбитків пальців. Програми середнього рівня пропонують більш широкий спектр функцій: гарантують повернення платежів, автоматичне відхилення підозрілих транзакцій, захист від нових способів шахрайств. Програми найвищого рівня захисту, попри те, що виконують всі ті самі функції, що й попередні, пропонують також аутсорсингові управління, автоматичне прийняття рішень і ручний перегляд підозрілих транзакцій, гарантуючи, що жодне замовлення не буде помилково відхилене.

Зауважимо, що журнал Merchant Fraud склав список кращих програм запобігання кібершахрайству, серед них: Kount, Riskified, Forter, Signifyd, ClearSale, CyberSource, Feedzai, Ravelin, Sift, Fraud.net, Nethone, Precognitive, SEON, FraudLabs Pro [195]. При оплаті відповідні програми автоматизують перевірки на шахрайство, здійснюють блокування підозрілих пристроїв, скасовують шахрайські замовлення й багато іншого. Вбачається за доцільне на прикладі Kount Identity Trust розглянути основний принцип роботи та функції таких програм. Передусім зазначимо, що Kount Command, коли споживач хоче придбати товар на сайті або в мобільному додатку, використовує штучний інтелект, оснащений контрольованим і неконтрольованим машинним обладнанням для аналізу попередньої комерційної діяльності цієї особи, порівнюючи наявні дані про особу з мільярдами інших взаємодій в Identity Trust Global Network в реальному часі. Такий аналіз встановлює рівень довіри до особистості потенційного споживача. Якщо буде виявлено високий рівень довіри, то компанія може схвалити угоду зі споживачем в одну мить, в іншому

випадку – відхилити угоду. Крім того, Kount Command запобігає шахрайству у сфері електронної торгівлі шляхом блокування шахрайства з новим акаунтом, з електронними подарунковими картками, цифровим платежем й зупиняє зловживання купонами й промоакціями [196].

Підсумовуючи, слід зазначити, що використання електронних систем запобігання шахрайству, а також електронних засобів контролю, - пріоритетний напрям політики ведення електронної комерційної діяльності. Вбачається, що першочерговими завданнями на сьогодні є: створення Єдиної інформаційної системи профілактики шахрайства у сфері електронної торгівлі, яка поєднуватиме різноманітні інформаційні ресурси, платформи й бази даних про шахраїв; проведення політики належного корпоративного управління; запровадження дієвих законодавчих ініціатив; реформування інституту кримінальної відповідальності; використання новітніх електронних систем і досягнень штучного інтелекту щодо запобігання електронному комерційному шахрайству; популяризація електронної комерції через онлайн та офлайн-магазини; посилення міжнародного співробітництва і залучення громадськості до соціально-виховної роботи з профілактики шахрайства у сфері електронної торгівлі.

3.2. Загальносоціальне та спеціально-кримінологічне запобігання шахрайству у сфері електронної торгівлі

Одним із головних завдань нашого кримінологічного дослідження є пошук заходів запобігання шахрайству у сфері електронної торгівлі, усунення причин й умов, які його породжують, а також сприяють його різноманітним проявам, створюючи тим самим реальні передумови поступового зниження суспільної небезпечності даного виду шахрайства і зменшення, врешті-решт, масштабів самої злочинності.

У Великій українській юридичній енциклопедії наведено визначення поняття «**запобігання злочинності**» – теорія та практика випереджального

впливу на злочинність шляхом перешкоджання дії чинників, які її детермінують, а також відвернення й припинення злочинних проявів на різних стадіях злочинної поведінки. Таке трактування видається цілком логічним, оскільки у процесі історичного розвитку людство поступово переконувалося в тому, що для ефективної протидії злочинності недоцільно впливати лише на тіло, плоть злочинця (жорстокі, нелюдські покарання), потрібно змінити й духовний стан людини, а цього можна досягти шляхом усунення тих різноманітних чинників, які посилюють людські пристрасті й зумовлюють суспільно небезпечну поведінку. Ще з давніх часів сформувалося розуміння того, що для більш-менш перспективної протидії злочинності потрібні не лише спеціальні, у т. ч. кримінально-правові, а й соціальні заходи з удосконалення суспільних відносин, культури, освіти, виховання, побуту, матеріального добробуту населення, самої людини, усунення негативних явищ і процесів у суспільстві. Наприклад, Платон висловлював думку, що злочин – це прояв дисгармонії, поганих схильностей людей, недосконалості законодавства, яке не відвертає особу від злочину. Він вважав, що однією з дійсних причин злочинності є недостатнє виховання, тому мета законодавця і стража законів зробити так, щоб людина стала доброчесною, полюбила справедливість. Науковою базою сучасної протидії злочинності передусім є теорія, що визначає рівні, масштаби, суб'єктів, об'єкти, різновиди запобіжної діяльності, заходи й засоби її здійснення, методологічне, методичне, інформаційне, організаційно-управлінське та інше ресурсне забезпечення.

Наголосимо на тому, що вітчизняна кримінологічна теорія залежно від природи й сфери дії детермінант злочинності та її злочинних проявів виходить із трирівневої системи запобіжних напрямів: **загальносоціальне**, **спеціально-кримінологічне** та **індивідуальне запобігання** [197, с. 153 - 154]. У межах цього підрозділу нашого дослідження розглянемо загальносоціальне і спеціально-кримінологічне запобігання шахрайству у сфері електронної торгівлі.

Як правило, основними цілями **загальносоціального запобігання** електронному комерційному шахрайству є подолання або обмеження криміногенно-небезпечних суперечностей у суспільстві, поступове викорінення відомих негативних явищ і процесів, зумовлених дією політичних, економічних, ідеологічних, психологічних, міжнаціональних та інших чинників, а також криміногенного потенціалу в суспільстві (йдеться про економічні й політичні кризи, небезпечне надмірне, навіть злочинне, збагачення певних кіл громадян, безробіття, затримка заробітної плати, існування на межі виживання переважної частини населення, занепад моралі, алкоголізм, наркоманія, безпритульність, непомірні тарифи на комунальні послуги та інші соціальні потреби) [197, с. 154], завдяки здійсненню непрямого превентивного впливу на детермінанти шахрайства у сфері електронної торгівлі та створенню передумов для вжиття ефективних заходів спеціального запобігання кримінальним правопорушенням проти власності.

Слід підкреслити, що вищенаведені положення стосовно загальносоціального запобігання злочинності підтверджують те, що передусім варто позбутися передумов поширення явища шахрайства у сфері електронної торгівлі й створити умови для зниження рівня соціальної напруги й недовіри між продавцями й споживачами товарів/послуг в мережі Інтернет. Для досягнення цієї мети потрібно докласти зусиль до того, щоб правовідносини між продавцями й покупцями товарів у сфері електронної торгівлі відбувалися виключно у законний спосіб, без порушення чинного законодавства і кримінально-правових посягань проти власності. Звісно, такі завдання виконуються на загальнодержавному рівні шляхом провадження ефективної економічної, соціальної та правової державної політики.

Ведучи мову про державну політику, відмітимо, що згідно з Національною економічною стратегією на період до 2030 р. місією керівництва України було визначено створення можливостей для реалізації наявного географічного, ресурсного й людського потенціалів країни для

забезпечення належного рівня добробуту, самореалізації, безпеки, прав і свобод кожного громадянина України через інноваційне випереджальне економічне зростання. Крім того, Стратегія закріплює основну економічну візію України, як: 1) вільної країни, в якій проживають громадяни з високим рівнем добробуту; 2) ефективної сервісної цифрової держави, яка є надійним економічним партнером у світі та прикладом розвитку для всіх країн Східного партнерства; 3) найпривабливішою країною економічних можливостей для інвестицій, інновацій, ведення бізнесу; 4) найкраще місце для реалізації творчого потенціалу, втілення ідей та власного розвитку [198].

Разом із тим дана Стратегія вказала основні орієнтири, принципи й цінності економічної політики в Україні, серед них: 1) європейська і євроатлантична інтеграція (реалізація стратегічного курсу держави на набуття повноправного членства України в ЄС і в Організації Північноатлантичного договору); 2) ефективна цифрова сервісна держава й компактні державні інститути (розвиток цифрової економіки як одного із драйверів економічного зростання України); 3) правова держава («недоторканна приватна власність»); 4) верховенство права (дотримання верховенства права під час реалізації державної політики); 5) захищеність прав усіх суб'єктів права власності; 6) нетерпимість корупції (запобігання й протидія будь-яким проявам корупції); 7) економічна свобода («підприємець – основа економіки»); 8) вільна і чесна конкуренція, рівний доступ для бізнесу; 9) розвиток підприємництва, інновацій і талантів; 10) без бар'єрного руху капіталу на території України; 11) інституційна спроможність («держава, що здатна забезпечити розвиток»); 12) інтегральний економічний підхід, спроможність ефективного єднання ліберальних та інституційних підходів; 13) національна безпека завдяки партнерству й інвестиціям [198].

На перший погляд, може здатися, що наведені цілі й напрями розвитку національної економіки мало стосуються зниження рівня загальнокримінальної злочинності в цілому й електронного комерційного

шахрайства зокрема. Проте досягнення вищезазначених цілей створює умови для розвитку технологічності бізнесу, електронної комерції та електронної торгівлі, а також підвищує рівень добробуту і платоспроможності населення, що позитивно впливає на відносини продавців і споживачів.

У зв'язку з тим, що «цифрові технології – це основа добробуту України; світ, де створюються нові можливості; сфера, що визначає суть трансформацій у країні для кращого життя, роботи, творчості та навчання», на окрему увагу заслуговує напрям «Цифрова економіка» Національної економічної стратегії на період до 2030 р. Акцентуємо на тому, що законодавець виокремив основні виклики й бар'єри на шляху до розвитку цифрової економіки України, а саме: 1) низький рівень проникнення технологій та загальної комп'ютеризації, недостатнє покриття фіксованим і мобільним Інтернетом; проблеми з покриттям 3G і 4G автомобільних доріг; 2) відсутність Національного плану розвитку широкосмугового доступу до Інтернету як документа, що визначає напрям розв'язання питань цифрового розриву між містом і селом; 3) інтероперабельність державних реєстрів, що потребує пришвидшення разом із суттєвою модернізацією самих реєстрів; 4) неврегульованість використання хмарних сервісів державними органами, переваг і ризиків (цифровий суверенітет); 5) недостатність правової бази стосовно хмарних технологій та інтероперабельності; 6) застарілість правової бази та стандартів безпеки технологій та інформації.

Водночас розв'язати вказані проблеми пропонується шляхом: 1) підвищення рівня покриття мобільним і фіксованим Інтернетом; 2) підвищення рівня комп'ютеризації об'єктів соціальної інфраструктури; 3) покращення системи хмарних послуг зі зберігання й обчислення; 4) оцифрування даних і підвищення інтероперабельності реєстрів; 5) імплементації та покращення сервісів електронної ідентифікації; 6) підвищення рівня кібербезпеки; 7) покращення сфери електронних платежів; 8) покращення інфраструктури й регулювання Індустрії 4.0; 9) стимулювання переходу на безготівкові

розрахунки; 10) стимулювання зростання електронної комерції, а саме забезпечення: а) розширення способів здійснення оплати й впровадження розрахунку електронними грошима; б) розвитку смартлогістики та супутніх послуг; в) сприяння розвитку транскордонної електронної торгівлі шляхом гармонізації відповідних стандартів та правової бази; г) проведення комплексного експертного аналізу законодавства України щодо імплементації Директиви 2000/31/ЄС про електронну комерцію; 11) посилення цифрової трансформації системи освіти; 12) підвищення рівня цифрових навичок громадян; 13) підвищення рівня професійних і спеціалізованих цифрових навичок; 14) посилення міжнародного обміну інформацією; 15) гармонізації цифрового законодавства; 16) включення до міжнародної цифрової інфраструктури; 17) затвердження й імплементації цифрових прав [198].

На додачу до всього вищезгаданого звернемо увагу на те, що, хоч Національна економічна стратегія на період до 2030 р. визначає ключові кроки для розвитку промисловості, агросектору, видобутку, інфраструктури, транспорту, енергетичного сектору, інформаційно-комунікаційних технологій, креативних індустрій і сфери послуг, враховує важливі наскрізні напрямки, як-от діджиталізація, «зелений» курс, розвиток підприємництва і збалансований регіональний розвиток, на превеликий жаль, вона не міститься концепції та візії державної політики у сфері електронної торгівлі.

Таким чином, ураховуючи те, що досліджуване явище є однією з форм кримінальної поведінки людей, результатом деформації правової свідомості та правової культури, доцільно розглядати загальносоціальні заходи запобігання шахрайству у сфері електронної торгівлі відповідно до раніше встановлених детермінант. Виходячи з того, що основні детермінанти цього явища випливають з об’єктивних соціально-економічних суперечностей та деформації правової свідомості значної частини населення, до **загальносоціальних заходів запобігання шахрайству у сфері електронної торгівлі** пропонуємо віднести:

1) зниження рівня бідності й економічної депривації в суспільстві;
2) створення умов для реального збільшення доходів населення України;
3) розроблення стратегії зменшення рівня безробіття;
4) проведення ефективної культурно-виховної й просвітницької роботи серед споживачів товарів і послуг у сфері електронної торгівлі.

Передусім підкреслимо те, що проблеми бідності останніми роками набувають не тільки місцевого, а й глобального характеру, стаючи одними з ключових проблемних зон і прерогативою дослідження в діяльності багатьох національних і міжнародних інституцій покликаних віднайти варіанти подолання бідності. Одним словом, бідність вважається однією з найболючіших проблем сучасного світу, від її зростання постійно страждає більшість населення нашого цивілізованого світу. Постійне підвищення рівня бідності суттєво впливає на розвиток людських можливостей, породжує масштабні соціальні й політичні протистояння, а у випадку відсутності швидкого реагування на появу загрози його виникнення може становити ризик цілісності суспільства, особливо у країнах з низьким показником економічного зростання [199, с. 85].

З метою розв'язання проблеми крайньої бідності, нерівності й несправедливості у вересні 2015 р. 193 держави – члени ООН ухвалили план досягнення спільного кращого майбутнього на найближчі 15 років. У центрі цього «Порядку денного 2030» 17 Цілей сталого розвитку, досягнення яких потребує безпрецедентних зусиль усіх секторів суспільства. Серед таких цілей важлива роль у загальносоціальному запобіганні шахрайству у сфері електронної торгівлі належить: 1) подоланню бідності в усіх її формах і повсюди; 2) подоланню голоду, досягненню продовольчої безпеки, поліпшенню харчування і сприянню сталому розвитку сільського господарства; 3) забезпеченню здорового способу життя і сприянню благополуччю населення; 4) забезпеченню всеосяжної якісної освіти для всіх; …7) забезпеченню доступу до недорогих, надійних, сучасних джерел енергії для всіх; 8) сприянню поступальному сталому економічному зростанню,

повній зайнятості й гідній оплаті праці для всіх; 9) створенню стійкої інфраструктури, сприянню сталій індустріалізації та інноваціям; … 12) забезпеченню переходу до раціональних моделей споживання і виробництва; … 17) зміцненню засобів здійснення й активізації роботи в рамках Глобального партнерства в інтересах сталого розвитку [200].

Принагідно додати, що у 2016 р. на виконання Плану заходів з імплементації Угоди про асоціацію між Україною та Європейським Союзом на 2014 – 2017 рр. КМУ схвалив Стратегію подолання бідності, якою визначив механізми запобігання їй і основні завдання, виконання яких дозволить розв'язати окреслену проблему до 2020 року. Зокрема, у документі основним стратегічним напрямом зниження рівня бідності було названо сприяння зростанню доходів населення від зайнятості й виплат у системі державного соціального страхування. Також передбачено забезпечення доступу населення до послуг соціальної сфери незалежно від місця проживання, мінімізації ризиків соціального відчуження сільського населення [201]. Однак, оцінюючи сьогоднішню ситуацію із бідністю в Україні, можемо констатувати, що втілення в життя закріплених Стратегією програмних заходів, цілей й завдань, не принесло очікуваних результатів.

На наше глибоке переконання, подолати вищевказану проблему в Україні можна шляхом комплексного вжиття наступних заходів: 1) створення сприятливих умов для росту ВВП і запровадження ефективного механізму його розподілу; 2) забезпечення зниження рівня безробіття; 3) підвищення рівня зайнятості працездатного населення; 4) посилення ефективності соціальної захищеності; 5) збільшення розміру мінімальної заробітної плати; 6) активізації співпраці між державою, громадськими організаціями й бізнесом з метою дотримання принципів соціального партнерства й солідарності; 7) забезпечення правильного розподілу державної соціальної допомоги; 8) реформування системи надання пільг; 9) врегулювання процесу трудової міграції; 10) покращення законодавчої бази та справедливості судової

системи; 11) розроблення довгострокової стратегії розвитку деструктивних регіонів [202, с. 91].

Крім того, що останніми роками підвищується рівень бідності, в Україні не відповідають потребам людей доходи, зокрема, їх основна складова – мінімальна заробітна плата, у тому числі розмір прожиткового мінімуму на одну особу, мінімально гарантований розмір пенсії. Такий стан справ спостерігається на тлі того, що протягом 2021 року зросли ціни на: освіту (на 16,8 %), продукти харчування (на 10,2 %), транспорт (на 10,0 %), житло, воду, електроенергію, газ та інші види палива (на 9,9 %), зв'язок (на 6,7 %), охорону здоров'я (на 5,0 %), предмети домашнього вжитку, побутову техніку й поточне утримання житла (на 4,1 %), відпочинок і культуру (на 3,5 %), одяг і взуття (на 2,2 %). З огляду на це середньомісячні сукупні витрати одного домогосподарства у І кварталі 2021 року склали 10 968 грн (у І кварталі 2020 року – 9 689 грн), міського – 11 262 грн, сільського – 10 350 грн (у І кварталі 2020 року – 10 045 грн та 8 945 грн відповідно) [202]. Виходячи з цього, можемо констатувати, що збільшення реального рівня доходів громадян можливе лише шляхом комплексної політики держави, яка повинна реалізовуватися, спираючись на довготривалий план дій щодо: 1) запровадження нових механізмів відновлення виробництва, стимулювання економічного зростання і соціального прогресу, зокрема, забезпечення ефективної зайнятості населення шляхом створення життєспроможних підприємств; 2) забезпечення реформування системи оплати праці, соціального захисту, пенсійного страхування, надання медичної допомоги, медичного обслуговування; 3) запровадження дієвого механізму надання молоді першого робочого місця; 4) вжиття в кризових умовах короткострокових заходів із надання невідкладної допомоги найбільш вразливим верствам населення тощо.

Зауважимо, що рівень доходів безпосередньо пов'язаний із зайнятістю населення. З цього приводу С. Т. Слюсар зазначає, що безробіття – найбільш

гостра проблема, з якою стикається населення України в умовах сьогодення, а причиною цього є неефективність використання робочої сили в минулому і відсутність економічних умов, які дали змогу б людям застосовувати свої навички у продуктивній роботі за гідну плату. Саме тому безробіття є як економічною, так і соціальною проблемою, що набуло у нашій країні масового характеру і становить реальну загрозу державному й суспільному благополуччю [203, с. 85].

Звісно, так не має бути, тим більше, що певне підґрунтя для покращення ситуації вже закладено. Нагадаємо, що відповідно до ст. 16 Закону України від 5 липня 2012 р. № 5067-VI «Про зайнятість населення» держава забезпечує реалізацію політики у сфері зайнятості населення шляхом: 1) проведення податкової, кредитно-грошової, інвестиційної, бюджетної, соціальної, зовнішньоекономічної та інноваційної політики з метою розширення сфери застосування праці, забезпечення повної, продуктивної, вільно обраної зайнятості, підвищення рівня кваліфікації та конкурентоспроможності робочої сили; 2) визначення у загальнодержавних програмах економічного й соціального розвитку, програмах економічного й соціального розвитку Автономної Республіки Крим, областей, районів, міст показників розширення ринку праці й зайнятості населення, їх оцінювання за результатами реалізації таких програм; 3) включення до системи регулювання ринку праці заходів щодо запровадження стимулювання вітчизняного виробництва до створення нових робочих місць у пріоритетних галузях економіки й сільській місцевості; 4) сприяння підвищенню конкурентоспроможності робочої сили й зайнятості населення; 5) соціального захисту громадян у разі настання безробіття; 6) сприяння самозайнятості населення шляхом стимулювання відкриття власного бізнесу, у тому числі в сільських населених пунктах та на депресивних територіях; 7) розвитку сільського аграрного туризму, кластерів народних художніх промислів; 8) створення умов для забезпечення підвищення конкурентоспроможності робочої сили та її мобільності; 9)

прогнозування та оцінки впливу на ринок праці політики у сфері зайнятості; 10) ліцензування діяльності з посередництва у працевлаштуванні за кордоном [204].

Крім того, у розпорядженні КМУ від 24 грудня 2019 р. № 1396-р «Про затвердження Основних напрямів реалізації державної політики у сфері зайнятості населення та стимулювання створення нових робочих місць на період до 2022 року» наведено чіткий перелік напрямів і шляхів розв'язання проблеми безробіття, серед них: 1) розвиток національної економіки як основи для забезпечення продуктивної зайнятості та створення нових робочих місць; 2) стимулювання розвитку підприємництва й самозайнятості; 3) забезпечення створення гідних умов праці й детінізація відносин у сфері зайнятості населення; 4) розвиток системи професійної (професійно-технічної) освіти та забезпечення створення умов для професійного навчання впродовж життя; 5) забезпечення розвитку інклюзивного ринку праці; 6) сприяння зайнятості молоді; 7) реформування державної служби зайнятості та забезпечення інноваційного розвитку послуг на ринку праці; 8) забезпечення реалізації ефективної державної політики у сфері трудової міграції [205].

Вбачається, що для подолання безробіття потрібно: 1) запровадити механізми захисту внутрішнього ринку праці країни; 2) реалізувати державні й регіональні програми зайнятості населення; 3) знизити податки для підприємств за умови збереження робочих місць; 4) застосувати економічні стимули фінансово-кредитного механізму для створення інвестиційного клімату й ефективного ринкового середовища; 5) сформувати легалізацію тіньової зайнятості; 6) забезпечити розвиток сільського господарства через вдосконалення системи збуту продукції [203, с. 90].

Вважаємо за доцільне звернути увагу на поширення серед політичного істеблішменту і громадян правового нігілізму, інфантилізму й ідеалізму – основних деформацій правової свідомості й культури, притаманних перехідним суспільствам через не сформованість правових знань або

ігнорування норм закону [206, с. 212]. Це вимагає негайного вжиття заходів, спрямованих на змінення культурних, моральних й етнічних засад суспільного життя. До речі, Л. М. Герасіна з цього приводу зазначає, що під видами деформації правосвідомості можна розуміти способи її прояву, які відрізняються один від одного різним ступенем перекручення компонентів правової свідомості у віддзеркаленні правової дійсності та які в сукупності розкривають суть і зміст цього явища. Усі види деформації правосвідомості – правовий нігілізм, правовий ідеалізм (фетишизм), правовий інфантилізм, правовий дилетантизм, правова демагогія, правовий скептицизм і «переродження» правосвідомості – торкаються перш за все деформації індивідуальної правосвідомості, що не виключає їх прояву на груповому й суспільному рівнях [206, с. 218].

Оскільки правосвідомість та правова культура населення є соціальною гарантією дії принципу верховенства права в суспільстві, єдиним чинником, здатним утворювати державу й правопорядок, приводячи в дію Конституцію України й законодавство; то вони, відповідно, потребують постійного раціонального формування, вдосконалення, позитивного соціального розвитку. У сучасній науковій літературі вчені виокремлюють різноманітні шляхи формування правосвідомості й правової культури українських громадян, як-от: 1) демократизація всіх сфер соціального життя; 2) вдосконалення правотворчого й правозастосовчого процесів; 3) зміцнення законності й правопорядку; 4) розвиток правовідносин; 5) підвищення ефективності діяльності всієї системи правосуддя; 6) адаптація законодавства України до міжнародних норм і стандартів прав людини; 7) гармонізація законодавства України із нормативними актами Європейського Союзу.

Як стверджує філософиня Г. П. Клімова, для формування правосвідомості й правової культури важливе значення мають правове виховання й правове навчання українських громадян, а також підвищення ефективності їх правової інформованості. Учена переконана, що правове

виховання спрямоване на перетворення правових ідей та вимог на особисті переконання громадян і норму їх поведінки, розвиток їх правової культури та соціально-правової активності, навичок правомірної поведінки. Звідси випливає, що правове виховання покликано сформувати такі якості у людини, як-от: 1) знання місця права в суспільстві, його значення, напрямків і принципів правового регулювання; 2) знання норм та інститутів різних галузей права в межах, необхідних для побутової, навчальної, трудової, суспільної діяльності; 3) навички застосування права в конкретних ситуаціях, комплексні характеристики варіантів вчинків не тільки як правильних чи неправильних, поганих чи хороших, а й законних і незаконних; 4) ставлення до права як до високої соціальної цінності - носія ідеї справедливості; 5) ставлення до правозастосовчої практики як до забезпечення життя закону; 6) внутрішня готовність до дотримання правових принципів і конкретних вимог правомірної поведінки; 7) готовність сприяти правомірній поведінці інших осіб [207, с. 309 - 310].

Розглянувши загальносоціальне запобігання шахрайству у сфері електронної торгівлі, перейдемо до **спеціально-кримінологічного**. Проте спершу викладемо загальні положення кримінологічної теорії запобігання злочинності.

У юридичній літературі, у тому числі у підручниках з кримінології, і на практиці для визначення діяльності із запобігання злочинності вживаються різні терміни: «**боротьба**», «**контроль**», «**профілактика**», «**протидія**». Так, В. І. Шакун спеціально-кримінологічне запобігання визначає як систему протидії злочинності та її проявам, змістом якої є різноманітна діяльність держави та її інституцій, пов’язана з усуненням детермінант, що породжують окремі види злочинів, а також недопущення їх учинення на різних стадіях злочинної поведінки, тобто на стадіях виникнення злочинної мотивації, готування до злочину та замаху на злочин [197, с. 154].

Однією з найбільш переконливих, на наш погляд, видається позиція Б. М. Головкіна, який зазначає, що головним завданням кримінологічної науки

є розроблення науково-обґрунтованих рекомендацій щодо боротьби зі злочинністю, яка включає державну політику, антикримінальне законодавство, комплекс заходів впливу на причини й умови злочинності та злочинної поведінки, притягнення злочинців до кримінальної відповідальності, виконання кримінальних покарань, міжнародну співпрацю у сфері забезпечення правопорядку, тобто як родове поняття боротьба зі злочинністю складається із запобігання правопорушенням, передовсім злочинам, і протидії злочинності. Крім того, учений запобігання кримінальним правопорушенням розглядає як систему заходів, спрямованих на виявлення й усунення причин і умов, що сприяють вчиненню злочинів, а також позитивний вплив на поведінку осіб, схильних до вчинення кримінальних правопорушень. Метою запобігання кримінальним правопорушенням є недопущення їх вчинення. Якщо запобігти вчиненню злочинів не вдалося, тоді починається протидія їм [208, с. 174 - 175].

У цілому відповідно до термінологічного словника понятєвого апарату сучасної кримінології, **спеціально-кримінологічне запобігання злочинності** – це сукупність заходів, що вживаються правоохоронними та іншими державними органами, громадськими організаціями й окремими громадянами з метою усунення причин і умов, що сприяють вчиненню злочинів, і недопущення їх вчинення на різних стадіях [209, с. 159].

За класичною кримінологією, до основних елементів запобігання злочинності учені відносять: об’єкти, суб’єктів, цілі й заходи запобіжної діяльності. Отже, розглянемо основні елементи запобігання шахрайству у сфері електронної торгівлі.

По-перше, В. В. Голіна підкреслює, що **об’єктом запобіжного діяння** є окремі негативні явища і процеси реальної дійсності матеріального й духовного характеру (або їх сукупність), різні за генезом, сферою, формами й інтенсивністю проявів, які, взаємодіючи з властивостями особистості, призводять до виникнення кримінальної мотивації, наміру, прийняття рішення

на вчинення кримінального правопорушення і його реалізацію [210, с. 49]. Виходячи з теми дослідження, можемо констатувати, що об'єктами запобіжного впливу є детермінанти злочинності у сфері електронної торгівлі, на які й слід спрямувати запобіжні заходи.

Враховуючи ці положення, пропонуємо об'єкти запобігання шахрайству у сфері електронної торгівлі поділити на загальні, спеціальні й індивідуальні. До **загальних** відносимо обставини, які мають зовнішній для розглядуваної злочинності характер (сукупність криміногенних явищ і процесів, пов'язаних із причинами й умовами вчинення кримінального правопорушення), зокрема, серйозні суперечності в розвитку економіки й пов'язані з цим зниження привабливості ведення електронного бізнесу в сегменті легальної економіки, складне соціально-економічне становище значної частини населення, недосконаліть нормативно-правової бази у відповідній сфері тощо. **Спеціальними** об'єктами запобіжного впливу виступають суб'єкти господарювання, які провадять електронну торгівлю (онлайн-магазини, електронні торговельні площадки, ін.). Мова йде про підвищення спроможності цих суб'єктів запобігати, виявляти й припиняти досліджуване кримінальне правопорушення. Нарешті, до **безпосередніх** об'єктів запобіжного впливу, на нашу думку, належать дві категорії осіб: 1) потенційні злочинці; 2) потенційні жертви електронного комерційного шахрайства.

По-друге, **суб'єкт** – це носій предметно-практичної діяльності й пізнання, джерело активності, спрямованої на об'єкт запобігання. Більш детально суб'єктів запобігання шахрайству у сфері електронної торгівлі розглянемо у підрозділі 3.3.

По-третє, запобігання шахрайству у сфері електронної торгівлі передбачає досягнення конкретних **цілей**, а саме: 1) усунення й нейтралізація детермінант електронного комерційного шахрайства; 2) зменшення рівня латентних проявів досліджуваної шахрайської діяльності; 3) підвищення ефективності, покращення координації діяльності правоохоронних органів із

запобігання вчиненню такого шахрайства; 4) мінімізація проявів віктимної поведінки потенційних жертв-споживачів.

По-четверте, спеціально-кримінологічне запобігання кримінальним правопорушенням включає вжиття наступних **заходів**: 1) кримінологічної профілактики; 2) відвернення; 3) припинення кримінальних правопорушень. З огляду на це **кримінологічна профілактика** означає завчасне вжиття заходів, які здатні перешкодити появі небажаних явищ, подій, зв'язків, наслідків чогось. Передчасне вжиття заходів як певна предметна діяльність охоплює заходи щодо випередження виникнення криміногенних явищ і процесів, обмеження їх поширення, послаблення, усунення, а також захист осіб, матеріальних і духовних цінностей від можливих злочинних посягань. Залежно від того, на які криміногенні явища й процеси спрямовані профілактичні заходи, їх можна за принципом професіоналізації та спеціалізації згрупувати в окремі види профілактики, а саме: а) профілактику випередження; б) обмеження; в) усунення; г) захисту. Водночас в**ідвернення** злочинних проявів відбувається тоді, коли злочинна поведінка проходить етап від формування злочинного мотиву до початку виконання діяння, а от **припинення** кримінальних правопорушень розглядається в контексті кримінально-правової теорії розвитку злочинної діяльності – з моменту виявлення наміру на вчинення кримінального правопорушення до його повної реалізації, включаючи готування до злочину, замах на злочин і закінчений злочин [210, с. 23; 30; 35].

Проводячи паралель з напрацюваннями криміналіста С. В. Самойлова щодо розслідування шахрайств, учинених із використанням мережі «Інтернет», слід врахувати те, що шахрайство у сфері електронної торгівлі є специфічним явищем у сучасній злочинності, суть якого полягає в тому, що: а) фізичне місцезнаходження шахрая, як і засобів учинення злочину, переважно не збігаються з місцем перебування потерпілого і настанням негативних наслідків злочину (місцем завдання матеріальної шкоди), а за певних випадків такі обставини можуть мати навіть транснаціональний (трансконтинентальний)

характер; б) відсутня залежність пори року та інших сезонних проявів, які прямо впливали б на злочинну активність шахраїв [135, с. 13]. Зважаючи на вищенаведені особливості досліджуваного кримінального правопорушення, вважаємо, що основним заходом спеціально-кримінологічного запобігання шахрайству у сфері електронної торгівлі є кримінологічна профілактика, на яку звернемо особливу увагу у цьому підрозділі. У цілому спеціально-кримінологічні заходи запобігання шахрайству, що вчиняється у сфері електронної торгівлі, пропонуємо розглядати з урахуванням раніше виокремлених у підрозділі 2.2 детермінуючих чинників.

На підставі вищевідзначених детермінант, причин і умов злочинної поведінки до першочергових **заходів кримінологічної профілактики** електронного комерційного шахрайства відносимо:

1) розробку і прийняття нормативно-правового акту про розвиток українського сегмента Інтернету, включення до зазначеного закону положення про неприпустимість використання ІКТ у неправомірних цілях;
2) вдосконалення профільного законодавства у сфері електронної торгівлі;
3) організацію повноцінної взаємодії правоохоронних органів, підприємств, установ, організацій всіх форм власності, ЗМІ з метою проведення інформаційно-виховної роботи серед населення щодо основних положень кібербезпеки;
4) контроль і облік осіб, які схильні до вчинення вказаного типу кіберзлочину.

Отже, першочергово варто подбати про безпечний інтернет-простір. Українське законодавство у сфері спам-розсилок потребує негайного вдосконалення. Нагадаємо, що спам – це електронні, текстові та/або мультимедійні повідомлення, що без попередньої згоди (замовлення) користувачів неодноразово (понад п’ять повідомлень одному абоненту) надсилаються на їхні адреси електронної пошти або кінцеве (термінальне)

обладнання, крім повідомлень постачальника електронних комунікаційних послуг щодо надання ним електронних комунікаційних послуг або повідомлень від органів державної влади чи органів місцевого самоврядування з питань, що належать до їх повноважень [211].

Окремо варто зупинитися на тому, що українське законодавство містить суперечливі положення у цій сфері. З одного боку, ст. 19 Закону України «Про захист прав споживачів» від 12 травня 1991 р. № 1023-XII забороняє здійснювати постійні телефонні, факсимільні, електронні або інші повідомлення без згоди на це споживача [212], а з другого – ст. 10 Закону України «Про електронну комерцію» дозволяє надсилати комерційні електронні повідомлення без згоди особи за умови, що в листі є кнопка «відписатися», тобто особа має можливість відмовитися від подальшого отримання таких повідомлень [91]. Здавалося б, що прийняття Закону України «Про електронні комунікації» від 1 січня 2022 р. № 2240-IX повинно було розв'язати вказану проблему, встановивши пряму заборонену умисного масового (понад п'ять повідомлень одному абоненту) розсилання спаму, крім повідомлень телеком-операторів, пов'язаних із наданням послуг, а також особистих повідомлень, які не носять масового характеру і мають некомерційну мету (ст. 120) [213]; проте аналіз згаданого нормативно-правового акту дає можливість зрозуміти, що законодавець не встановив відповідальності за порушення цієї норми. Так, згідно з положеннями Закону постачальник не несе відповідальності за зміст переданої чи отриманої інформації й за шкоду, завдану внаслідок використання результатів послуг, за умови, що він не є ініціатором передачі такої інформації, не обирає її отримувача і не може змінити її вміст (ст. 9). Більш того, цей нормативно-правовий акт не визначає правового статусу регуляторного органу у сфері зв'язку та інформатизації – Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ) [214]. Таким чином, відповідний Закон не містять дієвих механізмів, використання яких забезпечувало б беззастережне виконання вказаних заборон. Вочевидь, існує нагальна потреба закріпити обов'язок отримання попередньої згоди користувача

на використання його персональних даних із метою прямого маркетингу, заборонити практику надсилання повідомлень у цілях прямого маркетингу, які приховують ідентифікацію відправника або не мають дійсної адреси електронної пошти, передбачити дієві механізми відповідальності [215]. Крім того, деякі вчені пропонують розробити технологію інтернет-паспорта користувача, вважаючи, що це стане найбільш перспективною технологією, яка значно зменшить можливості поширення шахрайства у глобальній мережі Інтернет. Для реалізації подібних проєктів необхідно забезпечити належне фінансування вітчизняних науково-технічних досліджень і розвивати міжнародне співробітництво.

Ураховуючи те, що Закон України «Про електронну комерцію» містить чимало недоліків і неузгодженостей, про які йшлося в підрозділі 2.2, вважаємо, що найбільш важливим заходом кримінологічної профілактики шахрайства у сфері електронної торгівлі є вдосконалення профільного законодавства. Беремо сміливість стверджувати, що законодавцю необхідно: 1) надати коректні, повні, чіткі визначення понять «електронна комерція», «електронна торгівля» «інтернет-магазин», «інформаційні електронні послуги», «споживач», «електронний правочин»; 2) нормативно врегулювати порядок використання електронного підпису та/або електронного цифрового підпису; 3) визначити в Законі всі моделі електронної торгівлі, у тому числі B2B; 4) навести повний перелік об’єктів цивільних прав, які продавати із застосуванням ІКТ заборонено; 5) встановити порядок ідентифікації фізичної особи, яка не зареєстрована як фізична особа-підприємець і реалізує або пропонує до реалізації товари, виконує роботи, надає послуги з використанням ІКТ; 6) віднести до суб’єктів електронної комерції фізичних осіб, врегулювати захист прав таких споживачів і персональних даних; 7) охопити всі базові види електронних сервісів, віднести до них електронні сервіси міжнародної торгівлі; 8) розкрити принципи правового регулювання сфери електронної торгівлі, додати принцип свободи договору; 9) врегулювати питання обробки та зберігання даних із застосуванням хмарних технологій.

Наостанок зауважимо, що до заходів кримінологічної профілактики шахрайства у сфері електронної торгівлі інформаційно-виховного й віктимологічного характеру відносимо роз'яснювальну роботу правоохоронних органів (кіберполіції), підприємств, установ, організацій всіх форм власності (у тому числі банківських установ і закладів освіти), а саме: 1) інформування населення про появу нових випадків шахрайств при здійсненні купівлі-продажу товарів, виконанні робіт і наданні послуг у мережі Інтернет; 2) роз'яснення населенню всіх можливих способів захисту у сфері електронної торгівлі; 3) інформування громадян, підприємців, керівників фірм і підприємств про необхідність звертатися до правоохоронних органів при вчиненні шахрайств відносно них; 4) проведення бесід із населенням, особливо з молоддю, про наслідки вчинення шахрайства у сфері електронної торгівлі, а також роз'яснення правової культури використання інноваційних технологій. Вказані профілактичні дії повинні бути спрямовані на підвищення обізнаності населення, заклик громадян до обачності й перевірки тієї або іншої інформації при здійсненні купівлі-продажу в мережі Інтернет. На наш погляд, із метою поширення інформаційного контенту результативним є залучення до такої роботи ЗМІ. Важливо розміщувати роз'яснювальні матеріали під рубрикою «Як не стати жертвою шахраїв» і дані гарячих ліній кіберполіції, Національного банку України та інших відповідних служб у місцях прийому громадян, на біг-бордах постерів соціальної реклами, а також на сайтах і сторінках у соцмережах територіальних підрозділів правоохоронних органів, місцевих ЗМІ.

Зауважимо, що в контексті запобігання шахрайствам, які вчиняються шляхом використання засобів електронних комунікацій, слушною видається думка Л. В. Лефтерова щодо необхідності впровадження такого виду соціально-педагогічної профілактики у закладах середньої (середньо-спеціальної) і вищої освіти, як введення дисциплін щодо базових знань інформаційної безпеки й «ІТ-культури» (інформаційно-технічної). На переконання вченого, такі профілактичні дії мають бути спрямовані не лише на вивчення правил кібербезпеки, а й на зміну

девіантної поведінки на індивідуальному рівні, на обставини, які можуть зумовити таку поведінку [216, с. 97].

Також серед заходів недопущення збільшення кількості шахрайств у сфері електронної торгівлі дієвим є ведення обліку інформації стосовно осіб, схильних до вчинення вказаного виду кіберзлочину, з урахуванням вимог законодавства про інформацію і захист персональних даних і контроль за ними.

На закінчення додаємо, що на основі рекомендацій ПриватБанку – найбільшого за розмірами активів українського банку [217] і Olx – найбільшої вітчизняної платформи онлайн-оголошень ми розробили **основні правила безпеки купівлі-продажу в Інтернеті**.

Рекомендується:

1) користуватися складними паролями для входу в додаток інтернет-банкінгу або електронну пошту. Надійний пароль повинен містити: а) 8 або більше символів; б) хоча б одну велику літеру; в) хоча б одну маленьку літеру; с) хоча б одну цифру;
2) налаштувати двоетапну перевірку для входу в акаунт;
3) перевіряти з’єднання із сайтом в адресному рядку (https:// – золотий стандарт онлайн-безпеки);
4) встановлювати програмне забезпечення тільки з перевірених джерел;
5) стежити за тим, щоб на мобільному телефоні було встановлено й своєчасно оновлювалося антивірусне програмне забезпечення.
6) використовувати післяплату;
7) тим, хто веде бізнес, завести окремий контрактний телефон для переговорів зі споживачами, не використовувати фінансовий номер під час контактів із широким загалом.

Забороняється:

1) надавати інформацію про свої картки (CVV2-код, строк дії картки, баланс, тип картки) третім особам, навіть якщо вони звертаються нібито від імені банку;
2) зламувати операційну систему свого смартфона і проводити банківські операції через Інтернет на пристрої зі зламаною операційною системою;
3) відвідувати незнайомі або малознайомі сайти;
4) переходити на підозрілі посилання.

Отже, наведені вище заходи загальносоціального і спеціально-кримінологічного запобігання покликані мінімізувати й обмежити вплив окремих явищ суспільного життя, які зумовлюють вчинення шахрайства у сфері електронної торгівлі, зменшити рівень латентних проявів такої злочинності, підвищити ефективність, покращити координацію діяльності правоохоронних органів із запобігання вчинення шахрайства. Успішна реалізація запропонованих запобіжних заходів залежить від виваженої державної політики в забезпеченні нормального функціонування усіх сфер соціального життя суспільства.

3.3. Суб'єкти запобігання шахрайству у сфері електронної торгівлі

Останніми роками питання визначення кола суб'єктів, уповноважених запобігати шахрайству у сфері електронної торгівлі, залишається недостатньо розробленим. Тож, у цьому підрозділі перед нами постає завдання визначити перелік суб'єктів запобігання електронному комерційному шахрайству й основні напрямки їх діяльності. Разом із тим, зважаючи на специфічну запобіжну діяльність щодо зменшення кількості шахрайств у сфері електронної торгівлі, можна констатувати, що її проведення необхідно розглядати через призму статусу і повноважень суб'єктів запобігання такій злочинності.

Як правило, під **системою суб'єктів запобігання злочинності** слід розуміти сукупність з'єднаних єдиною метою суб'єктів, які виконують свої

повноваження у взаємозв'язку й за узгодженням у часі й просторі [36, с. 61]. Так, А. П. Закалюк наголошував, що **суб'єктами діяльності із запобігання злочинності й злочинним проявам** можуть бути визнані орган, організація, окрема особа, які у цій діяльності виконують хоча б одну з таких функцій щодо заходів запобігання: організація, координація, здійснення або безпосередня причетність до здійснення. Інші, зокрема забезпечуючі, заходи (навчання, видання літератури, підготовка рекомендацій, фінансування тощо) не дають функціональних підстав поширювати на їх виконавців термін «суб'єкт» запобігання злочинності та злочинним проявам [218, с. 129].

У цілому в межах цієї роботи вважаємо за доцільне дотримуватися позиції В. В. Голіни, який розкриває поняття «**суб'єкт запобігання злочинності**» як державний орган, громадську організацію, приватну установу, соціальну групу, службову особу чи громадянина, які спрямовують свою діяльність на розроблення та реалізацію заходів, пов'язаних з випередженням, обмеженням, усуненням криміногенних явищ і процесів, що породжують злочини, а також на їх недопущення на різних стадіях злочинної поведінки, у зв'язку з чим мають права, обов'язки та несуть відповідальність [36, с. 62].

Водночас ураховуючи ознаки електронного комерційного шахрайства, багатоманітність його проявів, можемо констатувати, що суб'єкти запобігання йому мають бути множинними, впливати на різні сфери життєдіяльності суспільства й перебувати у постійному взаємозв'язку для оперативного реагування на вчинення деструктивних дій, швидкого усунення наслідків і своєчасного притягнення винних до кримінальної відповідальності.

Крім того, відмітимо, що через низку прогалин в законодавстві щодо шахрайства у сфері електронної торгівлі, які унеможливлюють створення спеціальних органів запобігання такого виду кримінального правопорушення, і відсутність налагодженої, узгодженої, цілеспрямованої взаємодії між існуючими суб'єктами, що, у свою чергу, перешкоджає проведенню ефективної та своєчасної запобіжної діяльності з мінімізації вчинення

шахрайств у сфері електронної торгівлі, **система суб'єктів запобігання електронному комерційному шахрайству не є досконалою**.

Взагалі **суб'єктів запобігання шахрайству у сфері електронної торгівлі** в Україні з огляду на напрями їх діяльності, функції та повноваження **можна поділити на**:

1) суб'єктів, які визначають державну політику у сфері боротьби зі злочинністю (зокрема, запобігання кримінальним правопорушенням);
2) суб'єктів, які здійснюють координацію діяльності із запобігання кримінальним правопорушенням;
3) суб'єктів, які здійснюють правоохоронну діяльність у сфері боротьби зі злочинністю;
4) суб'єктів, діяльність яких напряму не пов'язана із запобіганням кримінальних правопорушень, водночас безпосередньо впливає на усунення їх причин та умов.

Оскільки шахрайство у сфері електронної торгівлі вчиняється у кіберпросторі[17], надалі з метою визначення кола суб'єктів запобігання йому будемо керуватися нормами Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [219].

Підкреслимо, що відповідно до ст. 8 вищевказаного Закону **національна система кібербезпеки** визначається як сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту

[17] Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», **кіберпростір** – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та / або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Виходячи з цього, **систему суб'єктів запобігання шахрайству у сфері електронної торгівлі складають**:

1) Верховна Рада України;
2) Президент України;
3) Кабінет Міністрів України, міністерства та інші центральні органи виконавчої влади;
4) органи місцевого самоврядування;
5) Державна служба спеціального зв'язку та захисту інформації України;
6) Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA;
7) Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України;
8) Національна поліція України (зокрема, Департамент кіберполіції Національної поліції України);
9) Національний банк України;
10) суб'єкти господарювання, громадяни України й об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Стисло схарактеризуємо кожного суб'єкта.

1. Суб'єкти, які визначають державну політику у сфері боротьби зі злочинністю. Так, переходячи безпосередньо до суб'єктів запобігання електронному комерційному шахрайству, мова перш за все піде про органи законодавчої влади. Конституцією України встановлено, що єдиним органом законодавчої влади в Україні є парламент – **Верховна Рада України** (ст. 75), до повноважень якої належить: 1) прийняття законів; 2) визначення засад

внутрішньої та зовнішньої політики, реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору; 3) затвердження загальнодержавних програм економічного, науково-технічного, соціального, національно-культурного розвитку, охорони довкілля; 4) надання законом згоди на обов'язковість міжнародних договорів України та денонсація міжнародних договорів України [79]. Отже, повноваження парламенту України дають йому підстави для розроблення головних напрямів боротьби зі злочинністю, створення достатньої правової бази для істотного впливу на кримінологічну політику держави, сприяти своєю діяльністю зниженню кількісно-якісних показників злочинності [210, с. 63]. Інакше кажучи, ВРУ приймає закони та інші нормативні акти у сфері електронної комерції, захисту прав споживачів, реклами, електронних документів та електронного документообігу, захисту інформації в інформаційно-телекомунікаційних системах, електронних комунікацій, електронного цифрового підпису, платіжних систем і переказу коштів в Україні, фінансових послуг і державного регулювання ринків фінансових послуг, захисту персональних даних тощо.

Підкреслимо, що до основних засад внутрішньої політики, які впливають на шахрайство у сфері електронної торгівлі та розглядаються як запобіжні, згідно із Законом України «Про засади внутрішньої і зовнішньої політики» від 1 липня 2010 року № 2469-VIII належить: 1) забезпечення життєвоважливих інтересів людини та громадянина, суспільства та держави, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національним інтересам у зовнішньополітичній, оборонній, соціально-економічній та інформаційній сферах; 2) забезпечення конкурентоспроможності національної економіки, досягнення високих темпів її зростання, забезпечення макроекономічної стабільності та низького рівня інфляції; 3) розвиток внутрішнього ринку, підвищення ефективності його функціонування та вдосконалення механізмів державного регулювання,

забезпечення збалансованості попиту та пропозиції на окремих ринках; 4) розвиток і зміцнення банківської системи й небанківських фінансових установ; 5) створення сприятливих умов для розвитку підприємництва, спрощення умов започаткування бізнесу і виходу з нього, зменшення втручання держави в економічну діяльність суб'єктів господарювання, спрощення системи отримання дозволів, зниження тиску на бізнес з боку контролюючих органів; 6) трансформація державної політики у сфері зайнятості та ринку праці, у тому числі шляхом розвитку партнерства між роботодавцями та найманими працівниками, власниками підприємств, установ, організацій та професійними спілками; 7) подолання бідності та зменшення соціального розшарування, зокрема, шляхом сприяння самозайнятості населення, розвитку малого та середнього бізнесу, недопущення виникнення заборгованості із заробітної плати на підприємствах, в установах, організаціях усіх форм власності [220].

Зауважимо, що ВРУ також здійснює контроль за дотриманням законодавства при вжитті заходів із забезпечення кібербезпеки у порядку, визначеному Конституцією України.

Наступним суб'єктом є **Президент України** як глава держави, гарант додержання Конституції України, прав і свобод людини та громадянина. Президент, приймаючи державні програми, створюючи відповідні інституції, на основі та на виконання Конституції та законів України, забезпечує запобігання злочинності та досягнення уповільнення темпів її динаміки на підставі чітко визначених пріоритетів, поступового нарощування зусиль держави й громадськості, вдосконалення законодавства та практики його застосування. У сфері кібербезпеки глава держави здійснює координацію діяльності як складової національної безпеки України через очолювану ним Раду національної безпеки і оборони України (далі РНБО), Національний координаційний центр кібербезпеки (далі НКЦК) як робочий орган РНБО; Кабінет Міністрів України та міністерства.

Ще одним суб'єктом визнається **КМУ** - вищий орган у системі органів виконавчої влади України. До його повноважень належить вжиття заходів щодо забезпечення прав і свобод людини та громадянина; розроблення і виконання загальнодержавних програм економічного, науково-технічного, соціального, культурного розвитку, а також розроблення, затвердження і виконання інших державних цільових програм; забезпечення розвитку та державної підтримки науково-технічного та інноваційного потенціалу держави; вжиття заходів щодо забезпечення національної безпеки України, громадського порядку, боротьби зі злочинністю (ст. 2 Закону України «Про Кабінет Міністрів України» від 4 лютого 2009 р. № 922-VI) [221]. До того ж згідно зі ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» у сфері запобігання кіберзлочинності, КМУ забезпечує формування й реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини й громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами та ресурсами функціонування національної системи кібербезпеки; формує вимоги й забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України) [219].

Крім КМУ, систему центральних органів виконавчої влади складають міністерства України та інші центральні органи виконавчої влади. Так, відповідно до Закону України «Про центральні органи виконавчої влади» від 12 грудня 2007 р. № 1185, міністерства забезпечують формування й реалізують державну політику в одній чи декількох сферах, а інші центральні органи виконавчої влади виконують окремі функції з реалізації державної політики [222]. Враховуючи те, що електронна торгівля – сфера цифрової економіки, суб'єктами запобігання електронному комерційному шахрайству, відповідно, є **Міністерство економіки України** (далі – Мінекономіки) та **Міністерство цифрової трансформації** (Мінцифри). Міністерства, відповідно до

покладених на них завдань, здійснюють забезпечення нормативно-правового регулювання; визначають пріоритетні напрямки розвитку; інформують і надають роз'яснення щодо здійснення державної політики; узагальнюють практику застосування законодавства, розробляють пропозиції щодо його вдосконалення і внесення в установленому порядку проєктів законодавчих актів, актів Президента України, КМУ на розгляд Президентові України й КМУ; забезпечують здійснення соціального діалогу на галузевому рівні, вживають заходи щодо боротьби із кіберзлочинністю.

Мінекономіки є головним органом у системі центральних органів виконавчої влади, що забезпечує формування й реалізує державну політику економічного, соціального розвитку і торгівлі, державну зовнішньоекономічну політику, державну політику у сфері технічного регулювання, стандартизації, метрології та метрологічної діяльності, розвитку підприємництва, інноваційної діяльності в реальному секторі економіки, а також державного замовлення на підготовку фахівців, наукових, науково-педагогічних і робітничих кадрів, підвищення кваліфікації та перепідготовку кадрів; державну політику у сфері захисту прав споживачів, державну політику з контролю за цінами, державну регуляторну політику; державну політику у сфері праці, зайнятості населення, трудової міграції, трудових відносин, соціального діалогу [223].

Аналогічно Мінцифри забезпечує формування й реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері розвитку цифрових навичок і цифрових прав громадян [224]. Ураховуючи те, що цифровізація визнається важливою складовою освітнього процесу України й водночас основою сталого розвитку суспільства та підвищення рівня життя громадян, Мінцифра розробила Портал «Дія. Цифрова освіта» для педагогічних й науково-педагогічних працівників, державних службовців,

підприємців і громадян, в основу якого покладено концептуальну еталонну європейську модель DigComp 2.1 й адаптовано до національних, культурних, освітніх та економічних особливостей України. Для прикладу, Рамка цифрових компетентностей для громадян України Цифрової освіти покликана покращити рівень цифрових компетентностей українців, допомогти у створенні державної політики та плануванні освітніх ініціатив, спрямованих на підвищення рівня цифрової грамотності й практичного використання засобів і сервісів ІТ-технологій конкретними цільовими групами населення.

Одночасно виконавчу владу на місцях (в областях і районах, містах Києві та Севастополі) здійснюють **місцеві державні адміністрації**, які в межах відповідної адміністративно-територіальної одиниці забезпечують виконання Конституції, законів України, актів Президента України, КМУ, інших органів виконавчої влади вищого рівня; законність і правопорядок, додержання прав і свобод громадян; виконання державних і регіональних програм соціально-економічного й культурного розвитку [225]; здійснюють державну політику у сфері запобігання злочинності.

Також серед суб'єктів запобігання злочинності важливе місце посідають **органи місцевого самоврядування** (далі ОМС), які за своїми повноваженнями здійснюють організаційно-управлінські функції щодо запобігання злочинності [210, с. 65 - 66]. У цілому місцеве самоврядування є правом територіальної громади – жителів села чи добровільного об'єднання у сільську громаду жителів кількох сіл, селища і міста – самостійно розв'язати питання місцевого значення в межах Конституції та законів України. Так, Основним Законом закріплено, що місцеве самоврядування здійснюється територіальною громадою в порядку, встановленому законом, як безпосередньо, так і через ОМС: сільські, селищні, міські ради та їх виконавчі органи (ст. 140). Одним словом, діяльність місцевого самоврядування спрямована не тільки на забезпечення інтересів громади в соціальній, економічній, правовій, культурній та побутовій сферах, а й на створення умов

безпечного життя, а також подолання негативних, антисуспільних, злочинних проявів.

2. Суб'єкти, які здійснюють координацію діяльності із запобігання шахрайству у сфері електронної торгівлі. Реалізація державної політики в галузі спеціального зв'язку й захисту інформації передусім покладена на **Державну службу спеціального зв'язку та захисту інформації України** (далі – Держспецзв'язок) – державний орган, призначення якого полягає в забезпеченні функціонування та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формуванні й реалізації державної політики у сферах криптографічного й технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку та ін. [226]. Так, Держспецзв'язок в межах своїх повноважень: 1) забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, і здійснює державний контроль у цій сфері; 2) координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; 3) забезпечує створення і функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; 4) здійснює організаційно-технічні заходи із запобігання, виявлення і реагування на кіберінциденти й кібератаки й усунення їх наслідків; 5) інформує про кіберзагрози та відповідні методи захисту від них; 6) забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України Computer Emergency Response Team of Ukraine (далі CERT-UA) [219].

Також до суб'єктів, для яких реагування на кібератаки та інші кіберзагрози є однією з головних функцій, належить **CERT-UA** – урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує у складі Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Серед основних завдань

урядової команди варто назвати такі, як: 1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; 2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення й усунення наслідків кіберінцидентів щодо цих об'єктів; 3) організація і проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; 4) підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; 5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; 6) взаємодія з іноземними й міжнародними організаціями з питань реагування на кіберінциденти; 7) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту та ін. [219]. Важливо зазначити, що з 2009 року CERT-UA є повноправним членом групи FIRST (Форум команд реагування на інциденти інформаційної безпеки), що об'єднує різні групи CERT в країнах світу. Це дає можливість в рамках протидії кіберзагрозам звернутися за підтримкою до будь-якої з 326 команд у 73 країнах [227].

Не можна оминути увагою й робочий орган РНБО, який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки й оборони у кіберпросторі та вносить Президентові України пропозиції щодо формування й уточнення Стратегії кібербезпеки України, – **НКЦК** при РНБО. Перш за все у Стратегії кібербезпеки України, прийнятій 26 серпня 2021 року, однією із найважливіших цілей визначено ефективну протидію кіберзлочинності. Відповідно до її норм Україна повинна забезпечити набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного й кадрового потенціалу для вжиття превентивних заходів і розслідування кіберзлочинів [228].

3. Суб'єкти, які здійснюють правоохоронну діяльність у сфері боротьби з шахрайством у сфері електронної торгівлі. До суб'єктів, для яких запобігання злочинності є однією з головних функцій у межах правоохоронної та правозастосовної діяльності, належать органи внутрішніх справ, їх підрозділи, відділи, служби й управління. Головним органом внутрішніх справ із забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки й порядку є **Національна поліція України**. У Законі України «Про Національну поліцію» від 2 липня 2015 р. № 580–VII прямо передбачено її основні завдання, зокрема: 1) здійснення превентивної та профілактичної діяльності, спрямованої на запобігання вчиненню правопорушень; 2) виявлення причин і умов, що сприяють вчиненню кримінальних і адміністративних правопорушень, вжиття в межах своєї компетенції заходів для їх усунення тощо [229].

Для виконання обов'язків з протидії кіберзлочинності, а також функції із запобігання їй, у 2015 році в поліції структурно було створено **Департамент кіберполіції** – міжрегіональний територіальний орган Національної поліції України, який входить до структури кримінальної поліції Національної поліції та забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність [230]. За словами А. Б. Ава-кова, кіберполіція була створена для реалізації державної політики у сфері: 1) протидії кіберзлочинності; 2) протидії кіберзлочинам у сферах використання платіжних систем, електронної комерції та господарської діяльності (фішинг, онлайн-шахрайство), інтелектуальної власності й інформаційної безпеки; 3) завчасного інформування населення про появу новітніх кіберзлочинів; 4) впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини; 5) реагування на запити закордонних партнерів, які надходять каналами Національної цілодобової мережі контактних пунктів; 6) участі у підвищенні кваліфікації працівників

поліції щодо застосування комп'ютерних технологій у протидії злочинності; 7) участі у міжнародних операціях і співпраці в режимі реального часу; 8) забезпечення діяльності мережі контактних пунктів між 90 країнами світу [231].

Керуючись інформацією, розміщеною на офіційному сайті Департаменту кіберполіції, можемо визначити його основні завдання щодо запобігання шахрайству у сфері електронної торгівлі, зокрема: 1) участь у формуванні й забезпеченні реалізації державної політики щодо попередження та протидії електронному комерційному шахрайству, механізм підготовки, вчинення або приховування якого передбачає використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку; 2) сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні й припиненні цього кримінального правопорушення [230]. З цього приводу не можна не погодитися з думкою М. С. Небеської та А. С. Салман, які стверджують, що запобігання злочинності ефективне лише тоді, коли воно закріплене законодавчо, і відповідна діяльність базується на міцній організаційній та науковій діяльності, тобто у своїй роботі працівникам органів поліції рекомендується використовувати інформацію про попередню протиправну і злочинну поведінку злочинця, причини й умови, що сприяють вчиненню таких злочинів, соціально-демографічні, морально-психологічні та кримінально-правові характеристики злочинця [232, с. 35–36].

4. Суб'єкти, діяльність яких напряму не пов'язана із запобіганням шахрайству у сфері електронної торгівлі, водночас безпосередньо впливає на усунення причин і умов відповідного кримінального правопорушення. Ураховуючи тісний взаємозв'язок електронної торгівлі й банківської системи, можна зробити висновок, що **Національний банк України** (далі – НБУ) відіграє чималу роль у процесах запобігання електронному комерційному шахрайству. Отже, НБУ, крім основних своїх завдань, визначає порядок, вимоги та заходи із забезпечення кіберзахисту й інформаційної безпеки у

банківській системі України та для суб'єктів переказу коштів, здійснює контроль за їх виконанням, створює центр кіберзахисту НБУ, забезпечує функціонування системи кіберзахисту у банківській системі України, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України [219].

Варто зауважити, що починаючи з 2020 р. НБУ разом із Департаментом кіберполіції Національної поліції України, а також за підтримки Міжнародної фінансової корпорації (IFC), у партнерстві з Державним секретаріатом Швейцарії з економічних питань (SECO), Фондом ефективного врядування Великої Британії та Мінцифрою України активно проводять Всеукраїнську інформаційну кампанію з платіжної безпеки під назвою «#ШахрайГудбай». Відповідна кампанія покликана покращити обізнаність громадян стосовно кібергігієни та правил безпеки безготівкових розрахунків, сприяти формуванню культури безпечної поведінки у віртуальному просторі, при купівлі-продажу товарів і послуг [233].

Поряд із цим до суб'єктів, діяльність яких напряму не пов'язана із запобіганням шахрайству у сфері електронної торгівлі, але безпосередньо впливає на усунення його причин й умов, належать **ЗМІ**. Загальновідомо, що Загальна декларація прав людини закріплює право людини на свободу переконань і на вільне їх виявлення. Це право включає свободу безперешкодно дотримуватися своїх переконань і свободу шукати, одержувати й поширювати інформацію та ідеї будь-якими засобами й незалежно від державних кордонів (ст. 19) [234]. Важливо, що діяльність ЗМІ, зокрема глобальної мережі Інтернет, сприяє підвищенню обізнаності та залученості громадян, а також розширенню доступу до інформації. У зв'язку з цим можемо констатувати, що ЗМІ виконують превентивну функцію у запобіганні шахрайству у сфері електронної торгівлі, стимулюючи правослухняну поведінку осіб, спонукаючи до соціального контролю, сприяючи усуненню віктимологічних станів і

«гальмуванню» механізмів злочинної поведінки, взаємодіючи з правоохоронними та судовими органами, іншими інституціями, які виконують кримінологічні функції [235, с. 69].

Однак слід звернути увагу на складний і неоднозначний механізм впливу ЗМІ на злочинність, оскільки інформація на злочинну тему може бути неповною, недостовірною, спотвореною, а самі повідомлення про вчинення кримінального правопорушення (зокрема, спосіб їх вчинення) можуть спонукати певні категорії осіб до вчинення кримінальних правопорушень.

Окремо звернемо увагу на те, що **суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом**, як суб'єкти запобігання шахрайству у сфері електронної торгівлі можуть: 1) створювати системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій; 2) сприяти підвищенню цифрової грамотності громадян і культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проєктів з підвищення рівня обізнаності суспільства щодо кіберзагроз і кіберзахисту; 3) надавати інформацію державним органам щодо кібератак та кіберінцидентів; 4) залучувати експертний потенціал, наукові установи, професійні об'єднання й громадські організації до підготовки ключових галузевих проєктів та нормативних документів у сфері кібербезпеки; 5) надавати консультативну й практичну допомоги з питань реагування на кібератаки; 6) формувати ініціативи й створювати авторитетні консультаційні пункти для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет; 7) запроваджувати механізм громадського контролю

ефективності заходів із забезпечення кібербезпеки; 8) створювати системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки [219].

Сутність вищевикладеного зводиться до того, що вивчення проблем, пов'язаних із взаємодією спеціальних органів держав щодо запобігання кіберзлочинності, і розробка сучасних механізмів протидії кіберзлочинності є одним з пріоритетних напрямків діяльності кожної держави. Безспірно, кіберзлочинність пов'язана безпосереднім причинно-наслідковим зв'язком з процесами глобалізації інформаційних процесів і появою глобальних телекомунікаційних мереж. Ефективна боротьба з кіберзлочинністю вимагає не лише гармонізації кримінального законодавства на міжнародному рівні, а й систематизації та адаптації комплексу процедурних заходів для співпраці щодо запобігання кіберзлочинам [236, с. 156].

Суб'єкти запобігання шахрайству у сфері електронної торгівлі є багатопрофільними, їх діяльність охоплює усі сфери суспільного життя. Однак на сьогодні невирішеним залишається питання створення вузькоспеціалізованого органу, відсутність якого знижує ефективність запобіжної роботи. Діяльність такого органу повинна бути спрямована на превентивну роботу досліджуваної злочинності. Тому дієвість заходів запобігання шахрайству у сфері електронної торгівлі можна забезпечити шляхом оновлення загальнодержавних і місцевих програм запобігання як усій злочинності, так шахрайству у сфері електронної торгівлі зокрема, вдосконалення кримінологічної політики держави з урахуванням потреб часу і модернізації адміністративних, оперативно-розшукових, охоронних, слідчих і запобіжних заходів боротьби зі злочинністю. Для успішної організації запобігання електронному комерційному шахрайству велике значення має правильно налагоджена взаємодія суб'єктів запобігання злочинності та чітке правове регулювання всіх видів і форм запобігання.

Крім того, за оцінками опитаних експертів, ефективнішому запобіганню шахрайству у сфері електронної торгівлі в роботі правоохоронних органів можуть сприяти впровадження наступних заходів:

1) налагодження (спрощення) обміну інформацією між операторами телекомунікаційних мереж і правоохоронними органами;
2) прив'язка телефонних номерів до паспорта громадянина;
3) підвищення кваліфікації працівників кіберполіції та збільшення забезпечення всім необхідним в їх роботи;
4) зменшення залежності правоохоронних органів;
5) надання прямого доступу до всіх державних реєстрів;
6) викорінення системи показників, яка губить якість роботи у складних справах.

Висновки до розділу 3

Встановлено, що явище шахрайства у сфері електронної торгівлі має масовий характер у США і країнах Азії (Китай, Індія, Південна Корея). Між тим, країни – лідери на світовому ринку електронної торгівлі визнають серйозну загрозу шахрайств, яка постає перед суб'єктами, що провадять електронну комерційну діяльність, і намагаються створити ефективні механізми її превенції.

Констатовано, що загальною тенденцію розвитку системи запобігання шахрайству у сфері електронної торгівлі у світі є регулярний аудит безпеки сайту, дотримання стандарту PCI DSS, регулярна перевірка сайту на підозрілу активність, постійне застосування служби перевірки адрес (AVS), CVV2, CVC2-кодів, безпечного протоколу передачі гіпертексту (HTTPS), зберігання обмеженої кількості інформації, перевірка IP-адрес, використання спеціальних програм для боротьби з шахрайством (Kount, Riskified, Forter, Signifyd, ClearSale, CyberSource, Feedzai, Ravelin, Sift, Fraud.net, Nethone, Precognitive, SEON, FraudLabs Pro тощо).

Аргументовано, що загальносоціальне запобігання явищу шахрайства у сфері електронної торгівлі має здійснюватися на основі політики покращення всі сфер життєдіяльності населення. Крім того, виокремлено наступні напрями цього рівня запобігання: 1) зниження показника бідності та економічної депривації в суспільстві; 2) створення умов для реального збільшення доходів населення України; 3) розроблення стратегії зменшення рівня безробіття; 4) здійснення ефективної культурно-виховної та просвітницької роботи серед споживачів товарів і послуг у сфері електронної торгівлі.

Наступним рівнем запобігання досліджуваним злочинам є спеціально-кримінологічний. Встановлено, що до заходів спеціально-кримінологічного запобігання шахрайству у сфері електронної торгівлі слід відносити: розробку й прийняття закону про розвиток українського сегмента Інтернету, включення до зазначеного закону положення про неприпустимість використання ІКТ у неправомірних цілях; вдосконалення профільного законодавства у сфері електронної торгівлі; організацію повноцінної взаємодії правоохоронних органів, підприємств, установ, організацій всіх форм власності, ЗМІ з метою проведення інформаційно-виховної роботи серед населення щодо основних положень кібербезпеки; контроль і облік осіб, які схильні до вчинення вказаного кримінального правопорушення.

Встановлено, що через відсутність законодавчого регулювання явища шахрайства у сфері електронної торгівлі, а також спеціальних органів запобігання цьому кримінальному правопорушенню і налагодженої, узгодженої, цілеспрямованої взаємодії між існуючими суб'єктами система суб'єктів запобігання електронному комерційному шахрайству не є досконалою.

Крім того, удосконалено класифікацію суб'єктів запобігання шахрайству у сфері електронної торгівлі шляхом поділу їх на: суб'єктів, які визначають державну політику у сфері боротьби зі злочинністю (зокрема, запобігання кримінальним правопорушенням); суб'єктів, які здійснюють

координацію діяльності у запобіганні шахрайству у сфері електронної торгівлі; суб'єктів, які здійснюють правоохоронну діяльність у сфері боротьби з шахрайством у сфері електронної торгівлі; суб'єктів, діяльність яких напряму не пов'язана із запобіганням шахрайству у сфері електронної торгівлі, водночас безпосередньо впливає на усунення причин і умов відповідного кримінального правопорушення.

ВИСНОВКИ

У дисертації вирішено наукове завдання, що полягає в дослідженні явища шахрайства у сфері електронної торгівлі, надано його кримінологічну характеристику, встановлено тенденції його поширення, особливості детермінації, на підставі чого розроблено рекомендації щодо запобігання такому виду кримінального правопорушення. На основі отриманих результатів зроблено наступні висновки та пропозиції.

1. З'ясовано, що технічний прорив і глобалізація економіки позначилися на розвитку суспільства. У даних умовах шахрайство не зникає, воно змінюється. До чинників, що вплинули на цей процес, віднесено: 1) четверту промислову революцію; 2) перехід до цифрової економіки; 3) глобалізацію світового співробітництва й економіки; 4) діджиталізацію суспільства; 5) стрімкий розвиток ІКТ і глобальної мережі Інтернет; 6) перехід світових і національних банків на безконтактні операції; 7) зміну цінностей та функцій грошей. Визначено, що теоретико-методологічні засади запобігання різним видам економічного (фінансового) шахрайства висвітлювалися у роботах багатьох вітчизняних і зарубіжних учених, однак, не применшуючи значення і цінність праць науковців, варто зазначити, що вказана тематика потребує постійного емпіричного оновлення і теоретичного осмислення в галузі кримінології, особливо в частині вивчення шахрайства у сфері електронної комерції та торгівлі.

2. Схарактеризовано особливості правового регулювання електронної комерції та електронної торгівлі, розкрито моделі електронної комерції, визначено її основні переваги й недоліки. З'ясовано, що електронна торгівля в Україні знаходиться на вершині свого розвитку, що зумовлено, зокрема, пандемію COVID-19, чим створює сприятливі умови для вчинення шахрайств у цій сфері. Після аналізу генезису явища шахрайства запропоновано власне авторське визначення поняття «шахрайство у сфері електронної торгівлі» – заволодіння чужим майном або придбання права на майно шляхом обману чи

зловживання довірою, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки у сфері електронної купівлі-продажу, реалізації товарів дистанційним способом через вчинення електронних правочинів із використанням інформаційно-телекомунікаційних систем. Виокремлено характерні кримінологічно-значущі риси шахрайства у сфері електронної торгівлі, серед них: інтелектуальність, висока латентність, значне віктимологічне і психологічне наповнення «віддаленої» моделі взаємодії шахрая і жертви (групової жертви), глобальний характер, вчинення кримінального правопорушення у віртуальному часі й кіберпросторі.

3. Констатовано, що кримінологічна характеристика шахрайства у сфері електронної торгівлі ґрунтується на аналізі різноманітної статистичної та аналітичної інформації про рівень, структуру й динаміку шахрайств, вчинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки. На підставі проведеного аналізу вдалося встановити щорічне збільшення кількості шахрайств у сфері електронної торгівлі. Доведено, що зростання електронної торгівлі, особливо в умовах пандемії COVID-19, є наслідком збільшення кількості таких шахрайств. Попри загальне зменшення кількості шахрайств, вчинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки, рівень шахрайств у сфері електронної торгівлі продовжує зростати. Встановлено, що найчастіше шахрайство у сфері електронної торгівлі вчиняється у спосіб отримання повної (64 %) та часткової (23,3 %) переплат, шляхом обману або зловживання довірою. Визначено основні майданчики (площадки), на яких вчиняється досліджуване шахрайство, серед них: Aukro.ua, ВКонтакті, Однокласники, Olx.ua, Facebook, Instagram. Виявлено основні категорії товарів і послуг електронної комерції, якими псевдопродавці-шахраї приваблюють жертв, а саме: транспортні засоби та запчастини до них, косметика і парфумерія, одяг і взуття, оренда нерухомості, побутова техніка й електроніка, товари загального вжитку.

4. Встановлено причини й умови вчинення шахрайств у сфері електронної торгівлі. До головних соціально-економічних чинників, що впливають на рівень вчинення шахрайств у вказаній сфері, належать: лібералізація й глобалізація цифрової економіки, стрімкий перехід торгівлі з офлайн режиму в онлайн, викликаний коронавірусною кризою, низький рівень доходів, обмежена купівельна спроможність громадян, високі показники безробіття, марнотратство, звичка витрачати більше, ніж заробляєш, крайня нужденність у товарах повсякденного життя, дефіцит окремих категорій товарів. Серед організаційно-управлінських чинників найбільш позначається упровадження нових технологій, недосконаліть законодавства у сфері електронної торгівлі, недосконаліть нормативно-правової бази у сфері кібербезпеки та державного контролю за електронною торгівлею, низький рівень обізнаності у сфері кібербезпеки громадян. До морально-психологічних криміногенних чинників належать: деформація правових і моральних цінностей, низький рівень правосвідомості та правової культури, перехід від реального спілкування до віртуального, переважаючий емоційний інтелект людей, ігровий характер поведінки, домінування матеріальних цінностей над духовними, неповідомлення жертвами шахрайства про кримінальне правопорушення.

5. Результати дослідження потенційних жертв шахрайства у сфері електронної торгівлі вказують на вірогідність гіпотези, що, з одного боку, ймовірність стати жертвою електронного комерційного шахрайства вища у людей з високим рівнем довіри, у яких відсутнє або погано розвинене критичне мислення та яким не відомі сучасні способи шахрайства, а з іншого – високою віктимністю вирізняються особи, котрі мають гарну освіту (переважно вищу), ведуть активний спосіб життя, пізнають нові види діяльності, однак при цьому характеризуються як азартні й самовпевнені люди, які люблять ризик, вірять у щасливий випадок. Виявлено, що жертвам електронного комерційного шахрайства притаманні специфічні відмінні

характеристики, які охоплюють не скільки соціально-демографічні, а переважно морально-психологічні групові риси.

6. Узагальнено міжнародний досвід попередження шахрайств у сфері електронної торгівлі на прикладі світових лідерів – США та Китаю. Встановлено, що у країнах з високорозвиненою електронною комерцією, таких, як США або країни Азії (Китай, Індія, Південна Корея), особлива увага приділяється захисту суб'єктів, які провадять електронну комерційну діяльність, від загроз шахрайства (у тому числі попередженню та запобіганню такому виду кримінальним правопорушенням). На прикладі США розглянуто основі види електронного комерційного шахрайства, як-от: шахрайство з кредитними картками або шахрайство з платежами, партнерське шахрайство, шахрайство зі зворотним платежем, фішинг, шахрайство з перехопленням, тріангуляційне шахрайство. Встановлено, що в цивілізованому світі основний тягар профілактики шахрайств у сфері електронної торгівлі лежить на продавцях і споживачах. Констатовано, що загальною тенденцію розвитку системи запобігання шахрайству у сфері електронної торгівлі у світі є регулярний аудит безпеки сайту, дотримання стандарту PCI DSS, регулярна перевірка сайту на підозрілу активність, постійне застосування служби перевірки адрес (AVS), CVV2, CVC2-кодів, безпечного протоколу передачі гіпертексту (HTTPS), зберігання обмеженої кількості інформації, перевірка IP-адрес. З'ясовано, що у сфері попередження електронного комерційного шахрайства одночасно використовуються спеціальні програми для боротьби з шахрайством (Kount, Riskified, Forter, Signifyd, ClearSale, CyberSource, Feedzai, Ravelin, Sift, Fraud.net, Nethone, Precognitive, SEON, FraudLabs Pro тощо), які здійснюють перевірки геолокацій IP-адрес, адрес електронної пошти, відбитків пальців і блокують шахрайство.

7. Розроблено систему заходів із запобігання вчиненню шахрайств у сфері електронної торгівлі. Обґрунтовано, що запобігання вчиненню шахрайств у вказаній сфері необхідно розглядати як багаторівневу систему

державних і громадських заходів, спрямованих на усунення або нейтралізацію причин та умов вказаного кримінального правопорушення на загальносоціальному, спеціально-кримінологічному й індивідуальному рівнях. Загальносоціальне запобігання шахрайству у сфері електронної торгівлі пропонується здійснювати за такими напрямами: зниження рівня бідності й економічної депривації в суспільстві; створення умов для реального збільшення доходів населення України; розроблення стратегії зменшення рівня безробіття; здійснення ефективної культурно-виховної та просвітницької роботи серед споживачів товарів і послуг у сфері електронної торгівлі. Спеціально-кримінологічне запобігання електронному комерційному шахрайству охоплює комплекс заходів щодо розробки та прийняття концептуального закону про розвиток українського сегмента Інтернету, включення до зазначеного закону положення про неприпустимість використання ІКТ у неправомірних цілях; вдосконалення профільного законодавства у сфері електронної торгівлі; організації повноцінної взаємодії правоохоронних органів, підприємств, установ, організацій всіх форм власності, ЗМІ із метою проведення інформаційно-виховної роботи серед населення щодо основних положень кібербезпеки; контролю й обліку осіб, які схильні до вчинення вказаного типу кіберзлочину. Розроблено основні правила безпеки купівлі-продажу в Інтернеті.

8. Аргументовано, що суб’єкти запобігання шахрайству у сфері електронної торгівлі, є багатопрофільними, їх діяльність охоплює усі сфери суспільного життя. Розроблено класифікацію таких суб’єктів, тобто поділено їх на: суб’єктів, які визначають державну політику у сфері боротьби зі злочинністю (зокрема, запобігання кримінальним правопорушенням); суб’єктів, які здійснюють координацію діяльності із запобігання шахрайству у сфері електронної торгівлі; суб’єктів, які здійснюють правоохоронну діяльність у сфері боротьби з шахрайством у сфері електронної торгівлі; суб’єктів, діяльність яких напряму не пов’язана із запобіганням шахрайству у

сфері електронної торгівлі, водночас безпосередньо впливає на усунення причин і умов відповідного кримінального правопорушення. Наголошено, через відсутність чіткої та максимально повної нормативної регламентації явища шахрайства у сфері електронної торгівлі, що унеможливлює створення спеціальних органів запобігання такому виду кримінального правопорушення, і налагодженої, узгодженої, цілеспрямованої взаємодії між існуючими суб'єктами, що, своєю чергою перешкоджає проведенню ефективної та своєчасної запобіжної діяльності з мінімізації вчинення шахрайств у сфері електронної торгівлі, система суб'єктів запобігання електронному комерційному шахрайству не є досконалою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Словник української мови : в 11 тт. / за ред. І. К. Білодіда. Київ : Наук. думка, 1970 - 1980. Т. 11. 700 с.
2. «Правда Руська» Ярослава Мудрого: початок вітчизняного законодавства : навч. посібник / уклад. : Г. Г. Демиденко, В. М. Єрмолаєв. Харків : Право, 2017. 392 с.
3. Российское законодательство X – XX веков. Законодательство периода образования и укрепления Русского централизованного государства : в 9 т. / за ред. О. И. Чистякова. Москва : Юрид. лит., 1984. Т.2. 520 с.
4. Российское законодательство X – XX веков. Акты земских соборов : в 9 т. / за ред. О. И. Чистякова, А. Г. Манькова. Москва : Юрид. лит., 1985. Т. 3. 512 с.
5. Российское законодательство X - XX веков. Законодательство периода становления абсолютизма : в 9 т. / за ред. А. Г. Манькова. Москва : Юрид. лит., 1986. Т. 4. 512 с.
6. Наказ Катерини II. URL: https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D0%BA%D0%B0%D0%B7_%D0%9A%D0%B0%D1%82%D0%B5%D1%80%D0%B8%D0%BD%D0%B8_II (дата звернення: 11.04.2020).
7. Права, за якими судиться малоросійський народ 1743 р. Київ: Книга, 1997. 598 с.
8. Уложение о наказаниях уголовных и исправительных. URL: https://ru.wikipedia.org/wiki/%D0%A3%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BE_%D0%BD%D0%B0%D0%BA%D0%B0%D0%B7%D0%B0%D0%BD(дата звернення: 11.04.2020).%D0%B8%D1%8F%D1%85_%D1%83%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D1%8B%D1%85_%D0%B8_%D0%B8%D1%81%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D1%85 (дата звернення: 11.04.2020).

9. Кримінальне уложення Російської імперії 1903. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B5_%D1%83%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F_%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D1%97_%D1%96%D0%BC%D0%BF%D0%B5%D1%80%D1%96%D1%97_1903 (дата звернення: 11.04.2020).

10. Об отмене права частной собственности на недвижимости в городах : Декрет ВЦИК от 23.11.1917 г. URL: http://www.economics.kiev.ua/download/ZakonySSSR/data04/tex17323.htm (дата звернення: 12.04.2020).

11. Первые декреты советской власти. URL: https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B2%D1%8B%D0%B5_%D0%B4%D0%B5%D0%BA%D1%80%D0%B5%D1%82%D1%8B_%D1%81%D0%BE%D0%B2%D0%B5%D1%82%D1%81%D0%BA%D0%BE%D0%B9_%D0%B2%D0%BB%D0%B0%D1%81%D1%82%D0%B8 (дата звернення: 19.04.2020).

12. Кримінальний кодекс : Закон УРСР від 1 червня 1922 року. URL: https://textbooks.net.ua/content/view/1060/17/ (дата звернення: 12.04.2020).

13. Кримінальний кодекс : Закон УРСР від 22 листопада 1926 року. URL: https://ru.wikisource.org/wiki/%D0%A3%D0%B3%D0%BE%D0%BB%D0%BE%D0%B2%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81_%D0%A0%D0%A1%D0%A4%D0%A1%D0%A0_1926_%D0%B3%D0%BE%D0%B4%D0%B0/%D0%A0%D0%B5%D0%B4%D0%B0%D0%BA%D1%86%D0%B8%D1%8F_05.03.1926 (дата звернення: 12.04.2020).

14. Берзін П. С. Кримінальний кодекс УСРР 1922 р. *Вісник Асоціації кримінального права України*. 2017. № 1(8). С. 276-278.

15. Об охране имущества государственных предприятий, колхозов и кооперации и укреплении общественной (социалистической) собственности : Постановление ЦИК и СНК СССР от 07.08.1932 г. URL: https://ru.wikisource.org/wiki/%D0%9F%D0%BE%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%A6%D0%98%D0%9A_%D0%B8_%D0%A1%D0%9D%D0%9A_%D0%A1%D0%A1%D0%A1%D0%A0_%D0%BE%D1%82_7.08.1932_%D0%BE%D0%B1_%D0%BE%D1%85%D1%80%D0%B0%D0%BD%D0%B5_%D0%B8%D0%BC%D1%83%D1%89%D0%B5%D1%81%D1%82%D0%B2%D0%B0_%D0%B3%D0%BE%D1%81%D1%83%D0%B4%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D1%8B%D1%85_%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D1%80%D0%B8%D1%8F%D1%82%D0%B8%D0%B9,_%D0%BA%D0%BE%D0%BB%D1%85%D0%BE%D0%B7%D0%BE%D0%B2_%D0%B8_%D0%BA%D0%BE%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8. (дата звернення: 12.04.2020).

16. Кримінальний кодекс : Закон УРСР від 01.01.1961 р. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/KD0006.html (дата звернення: 13.04.2020).

17. Кримінальний кодекс України : Закон від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 13.04.2020).

18. Про судову практику у справах про злочини проти власності : Постанова Пленуму Верховного Суду України № 10 від 06.11.2009 р. URL: https://ips.ligazakon.net/document/VS090693 (дата звернення: 13.04.2020).

19. Ємельянов М. В. Поняття та види шахрайства за кримінальним кодексом України. *Питання кримінального права та кримінології.* 2011. № 6. С. 164-168.

20. Панов Н. И. Квалификация преступлений, совершаемых путем обмана. Харьков, 1980. 88 с.

21. Зубко Г. Шостий технологічний уклад: інфраструктурно-правовий аспект. *Підприємництво, господарство і право*. 2019. № 11. С. 218-229.

22. Політанський В. Концептуальні ідеї розвитку інформаційного суспільства. *Підприємництво, господарство і право*. 2017. № 4. С. 140-144.

23. Цифрова економіка : підручник за заг. ред. Т. І. Олешко, Н. В. Касьянова, С. Ф. Смерічевський та ін. Київ : НАУ, 2022. 200 с.

24. Карчева Г. Т., Огородня Д. В., Опенько В. А. Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. *Фінансовий простір.* 2017. № 3 (27). С. 13-21.

25. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. *Вісник Дніпропетровського університету.* Серія: Менеджмент інновацій. 2015. Т. 23, вип. 4. С. 9-18.

26. Концепції розвитку цифрової економіки та суспільства на 2018 – 2020 роки : розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 15.03.2022 року).

27. Тетерятник Б. С. Діджитизація та діджиталізація в контексті віртуалізації господарської діяльності. *Право та інновації.* 2018. № 3. С. 180–184.

28. Сучасні інформаційно-комунікаційні технології : навчальний посібник. Дніпро : НМетАУ, 2017. 230 с.

29. У 2021 році кількість користувачів Інтернету зросла до 4,9 мільярда. URL: https://pon.org.ua/novyny/9141-u-2021-roci-kilkist-koristuvachiv-internetu-zrosla-do-49-miljarda.html (дата звернення: 30.04.2022).

30. За рік карантину кількість українських користувачів у соцмережах зросла на 7 млн і досягла 60% населення. GlobalLogic. URL: https://www.ukrinform.ua/rubric-technology/2797152-v-ukraini-kilkist internetkoristuvaciv-zrosla-do-23-miljoniv.html (дата звернення: 30.04.2022).

31. Дивовижні статистики в Інтернеті і соціальних медіа в 2022 році. URL:

https://uk.wizcase.com/blog/%D0%B4%D0%B8%D0%B2%D0%BE%D0%B2%D0%B8%D0%B6%D0%BD%D1%96-%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B8-%D0%B2-%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D1%96/ (дата звернення: 30.04.2022).

32. «Мінфін» і Finance.ua нагородили найкращі фінустанови країни. FinAwards 2021. URL: https://minfin.com.ua/ua/2021/05/25/65275974/ (дата звернення: 01.05.2020).

33. Про затвердження Положення про електронні гроші в Україні : Постанова правління Національного банку України від 25.06.2008 р. № 178. URL: https://zakon.rada.gov.ua/laws/show/z0688-08#Text (дата звернення: 01.05.2020).

34. Про віртуальні активи : Закон України від 17.02.2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text. (дата звернення: 01.03.2022).

35. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»: Указ Президента України від 14 2021 р. URL : https://www.president.gov.ua/documents/4472021-40013.05.(дата звернення: 15.03.2022 року).

36. Кримінологія: Загальна та Особлива частини : підручник / за заг. ред. В. В. Голіни. Харків : Право, 2009. 288 с.

37. Про Концепцію державної політики у сфері боротьби з організованою злочинністю : розпорядженням Кабінету Міністрів України від 16 вересня 2020 р. № 1126-р. URL: https://zakon.rada.gov.ua/laws/show/1126-2020-%D1%80#Text (дата звернення: 01.03.2020).

38. Про організаційно-правові основи боротьби з організованою злочинністю : Закон України від 30.06.1993 р. № 3341-XII. URL: https://zakon.rada.gov.ua/laws/show/3341-12#Text (дата звернення: 01.03.2020).

39. Маслій І. В. Інституційний механізм протидії криміналізації економіки: кримінологічне дослідження : дис. ... канд. юрид. наук : спеціальність : 12.00.08. Одеса, 2015. 228 с.

40. Пивоваров В. В., Гончаренко Т. В. Окремі питання корпоративної екологічної злочинності. *Порівняльно-аналітичне право : електрон. наук. фахове вид.* 2015. № 4. URL: http://www.pap.in.ua/4_2015 /95.pdf (дата звернення: 03.05.2020).

41. Пивоваров В. В. Корпоративна злочинність у процесах транскордонного наркобізнесу. *Право і суспільство.* № 2. С. 219-223.

42. Бабенко А. М., Палій М. В. Крадіжка та шахрайство як види корисливих кримінальних правопорушень проти власності: соціально-правова та віктимологічна характеристика. *Юридичний науковий електронний журнал*. 2023. № 1. С. 564-568.

43. Бабенко А. М. Тактико-психологічні, кримінально-процесуальні, адміністративно-правові та оперативно-розшукові заходи профілактики і запобігання кримінальним правопорушенням. *Південноукраїнський правничий часопис*. № 1. 2021. С. 14-23.

44. Бабенко А. М., Гавловський В. Д., Гіда О. Ф., Галунько В. В. Спеціально-кримінологічне запобігання злочинності з використанням мережі Інтернет. *Підприємництво, господарство та право.* № 8. 2018. С. 186-190.

45. Лисодєд О. В. Кримінологічні проблеми шахрайства : дис... канд. юрид. наук : спеціальність : 12.00.08. Харків, 1999. 221 с.

46. Коваленко П. М. Запобігання шахрайству на фінансових ринках у біржовій торгівлі : дис... канд. юрид. наук : спеціальність : 12.00.08. Київ, 2005. 201 с.

47. Микитчик А. В. Кримінологічні засади запобігання шахрайству з нерухомістю : дис... канд. юрид. наук : спеціальність : 12.00.08. Київ, 2009. 213 с.

48. Пластун В. Л. Проблеми шахрайства та практика його усунення. Економіка : проблеми та практики : Зб. наукових праць. Вип. 254. Т. 6. 2009. 488 с.

49. Андрушко А. В., Нестерова І. А. Злочинність у сфері туристичного бізнесу: кримінологічна характеристика та запобігання : монографія. Ужгород: ТОВ «ІВА», 2016. 220 с.

50. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. В. Ю. Шепітька. Харків : Право, 2010. 168 с.

51. Луценко Ю. В., Макаренко Н. К. Виконання спеціального завдання з попередження та розкриття кримінально протиправної діяльності організованої групи чи злочинної організації, що вчиняють шахрайські та корупційні правопорушення. *Юридичний науковий електронний журнал.* 2023. № 7. С. 364-368.

52. Луценко Ю. В., Тарасюк А. В. Кібербезпека та інформаційна безпека: співвідношення понять. *Юридичний науковий електронний журнал*. 2022. Т. 9. С. 320-323.

53. Павлова Н. В. Особливості розслідування шахрайства, пов'язаного з відчуженням приватного житла : дис... канд. юрид. наук : спеціальність : 12.00.09. Дніпропетровськ, 2007. 223 с.

54. Іщук І. В. Початковий етап розслідування шахрайств у сфері страхування автотранспортних засобів : автореф ... канд. юрид. наук : спеціальність : 12.00.09 Київ, 2010. 20 с.

55. Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. ... д-ра юрид. наук : спеціальність : 12.00.09. Київ, 2010. 34 с.

56. Кришевич О. В. Кримінально-правова характеристика предмета шахрайства. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. Вип. 24. С. 183-191.

57. Золотар О. О. Інформаційні революції: соціально-правове значення. *Публічне право.* 2017. № 2. С. 40-46.

58. Борейко Н. М. Основні етапи становлення та розвитку електронної комерції. *Південноукраїнський правничий часопис*. 2009. № 2. С. 101-104.

59. Електронна комерція. URL: https://sites.google.com/site/elektronnakomercia05/istoria-rozvitku-elektronnoie-komerciie (дата звернення: 04.09.2020).

60. Електронна комерція (електронна комерція). URL: https://uk.economy-pedia.com/11032578-electronic-commerce-ecommerce (дата звернення: 04.09.2020).

61. Treese G. Winfield, Lawrence C. Stewart. Designing Systems for Internet Commerce. Addison-Wesley, 1998. 375 p.

62. Bryan A. Gardner, Blacks Law Dictionary. 7th Edition. St. Paul (Minn.): West Group, 1999. P. 269.

63. Задвірний Я., Орловська А. Використання можливостей електронної комерції у процесі ведення бізнесу. *Формування ринкової економіки в Україні : зб. наук. пр.* Вип. 18. Львів : Інтереко, 2008. С. 70–75.

64. Макарова М. В. Електронна комерція : посібник. Київ: Видавничий центр «Академія», 2002. 272 с.

65. Меджибовська Н. С. Електронна комерція : навч. посібник. Київ: Центр навчальної літератури, 2004. 384 с.

66. Плескач В. Л. Технології електронного бізнесу : монографія. Київ, 2004. 223 с.

67. Маєвська А. Електронна комерція і право : навч.-метод. посібник. Харків, 2010. 256 с.

68. Мілаш В. С. Договірні аспекти господарсько-виробничих відносин у сфері електронної комерції. *Економічна теорія та право.* 2016. № 1 (24). С. 87-99.

69. Виноградова О. В., Євтушенко Н. О., Крючок І. С. Електронна комерція в епоху діджиталізації суспільства. *Причорноморські економічні студії.* 2020. Вип. 53. С. 55-61.

70. Дмитрієва Н. О. Концептуальні засади розвитку електронної торгівлі в національній економіці : дис. ... канд. юрид. наук : спеціальність : 08.00.03. Київ, 2018. 329 с.

71. A European Initiative in the sector of Electronic Commerce : Commission communication of 18 April 1997. URL: http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=LEGISSUM:l3 2101 (дата звернення: 12.09.2020).

72. World Trade Organization WT/L/274 30 September 1998 (98-3738) Work Programme On Electronic Commerce / Adopted by the General Council on 25 September 1998. URL: https://www.wto.org/english/tratop_e /ecom_e/ecom_e.htm (дата звернення: 13.09.2020).

73. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998. URL: http://www.uncitral.org/pdf/english/te xts/electcom/05-89450_Ebook.pdf (дата звернення: 12.09.2020).

74. Новицький А., Позняков С. Сутність та зміст поняття «електронна торгівля». *Правова інформатика*. 2007. № 1. С. 7-13.

75. Про правову охорону комп'ютерних програм : Директива Ради Європейського співтовариства від 14.05.1991 р. № 91/250/ЄЕС. URL: https://zakon.rada.gov.ua/laws/show/994_065#Text (дата звернення: 14.09.2020).

76. Про захист прав споживачів в дистанційних контрактах : Директива Європейського парламенту та Ради від 20.05.1997 р. № 97/7/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_245#Text (дата звернення: 14.09.2020).

77. Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі : Директива

Європейського Парламенту і Ради від 15.12.1997 р. № 97/66/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_243#Text (дата звернення: 15.09.2020).

78. Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку : Директива Європейського парламенту та Ради від 08.06.2000 р. № 2000/31/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_224#Text (дата звернення: 15.09.2020).

79. Конституції України : Закон України від 28.06.1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 15.09.2020).

80. Цивільний кодекс : Закон України від 16.01.2003 року № 435-IV. URL: https://ips.ligazakon.net/document/T030435 (дата звернення: 15.09.2020).

81. Господарський кодекс України : Закон України від 12.11.2019 року № 436-IV. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text (дата звернення: 16.09.2020).

82. Про захист прав споживачів : Закон України від 12.05.1991 року № 1023-XII. URL: https://zakon.rada.gov.ua/laws/show/1023-12#Text (дата звернення: 16.09.2020).

83. Про рекламу : Закон України від 18.11.1997 року № 642/97-ВР. URL: https://ips.ligazakon.net/document/view/z960270?ed=1999_06_30 (дата звернення: 16.09.2020).

84. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 року № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 16.09.2020).

85. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 04.06.2020 року № 681-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 16.09.2020).

86. Про телекомунікації : Закон України від 18.11.2003 року № 1280-IV. URL: https://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення: 16.09.2020).

87. Про електронні довірчі послуги : Закон України від 05.10.2017 року № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 16.09.2020).

88. Про платіжні послуги : Закон України від 30.06.2021 року № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text (дата звернення: 16.09.2020).

89. Про фінансові послуги та державне регулювання ринків фінансових послуг : Закон України від 12.07.2001 року № 2664-III. URL: https://zakon.rada.gov.ua/laws/show/2664-14#Text (дата звернення: 16.09.2020).

90. Про захист персональних даних : Закон від від 01.06.2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 16.09.2020).

91. Про електронну комерцію : Закон України від 03.09.2015 року № 675-VIII. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 13.09.2020).

92. Писаренко Н. Л., Євдокимова З. Р. Особливості функціонування та моделі бізнесу на ринку електронної комерції в Україні. *Економічний вісник Національного технічного університету України Київський політехнічний інститут.* 2017. №. 14. С. 348-355.

93. Електронна комерція. URL: https://psm7.com/news/aziatsko-tixookeanskij-region-lidiruet-v-globalnoj-e-commerce.html (дата звернення: 20.09.2020).

94. Світовий e-commerce і m-commerce – статистика і факти електронної комерції 2020. URL: https://marketer.ua/ua/e-commerce-worldwide-statistics-facts/ (дата звернення: 20.09.2020).

95. Основні тренди електронної комерції в 2020 році. URL: https://www.broadbandsearch.net/ (дата звернення: 17.10.2020).

96. Kantar Рейтинг популярних сайтів за січень 2022. URL: https://web.archive.org/web/20220316193405/https://tns-ua.com/news/reyting-populyarnih-saytiv-za-sichen-2022 (дата звернення: 11.03.2022).

97. OLX. URL: https://uk.wikipedia.org/wiki/OLX (дата звернення: 16.10.2020).

98. Prom.ua. URL: https://uk.wikipedia.org/wiki/Prom.ua (дата звернення: 16.10.2020).

99. Пандемія COVID-19 пришвидшила розвиток електронної комерції на п’ять років – звіт. URL: https://ms.detector.media/trendi/post/25338/2020-08-25-pandemiya-covid-19-pryshvydshyla-rozvytok-elektronnoi-komertsii-na-pyat-rokiv-zvit/ (дата звернення: 16.10.2020).

100. Електронна комерція в світі продовжує рости. URL: https://www.aciworldwide.com/ / (дата звернення: 23.10.2020).

101. Gradus Research. URL: https://gradus.app/documents/73/GradusReport_Online_shopping.pdf (дата звернення: 21.10.2021).

102. Ховрак І. В. Електронна комерція в Україні: переваги та недоліки. *Економіка. Фінанси. Право.* 2013. № 4. С. 16-20.

103. The True cost of Fraud™ Study | LexisNexis Risk Solutions. URL: https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study (дата звернення: 17.10.2020).

104. Науково-практичний коментар до Кримінального кодексу України / за ред. С. С. Яценко. Київ., 2005. 848 с.

105. Юристконсульт: народний правовий портал. URL: https://legalexpert.in.ua/komkodeks/uk/81-uky/1875-190.html (дата звернення: 01.11.2020).

106. Кримінальний кодекс України. Науково-практичний коментар : у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, В. І. Борисова, В. І. Тютюгіна. 5-те вид., допов. Харків : Право, 2013. 1040 с.

107. Чернишов Г. М. Фінансове шахрайство в інвестиційно-будівельній сфері: кримінологічне дослідження : дис. ... канд. юрид. наук : спеціальність : 12.00.08. Одеса, 2016. 246 с.

108. Головкін Б. М. Кримінологічний аналіз злочинів проти власності. *Теорія і практика правознавства : електр. наук. фах. вид.* 2013. Вип. 2. С. 1-10.

109. Пивоваров В. В. Податкова і кредитно-фінансова злочинність: кримінологічна характеристика та попередження : дис. … канд. юрид. наук : спеціальність : 12.00.08. Харків, 2003. 299 с.

110. Тихонова О. В. Щодо розуміння категорії «кримінологічна характеристика». *Науковий вісник Міжнародного гуманітарного університету.* 2014. № 8. С. 246-249.

111. Гула Л. Ф. Кримінологічна характеристика злочинів, учинених засудженими в установах виконання покарання. *Науковий вісник Львівського державного університету внутрішніх справ.* 2017. Вип. 3. С. 131-139.

112. Кримінологія. Особлива частина : навч. посіб. для студентів юрид. спец. вищих закладів освіти / за ред. І. М. Даньшина. Харків : Право, 1999. 232 с.

113. Кальман О. Г. Злочинність у сфері економіки України: теоретичні та прикладні проблеми попередження : дис. … д-ра юрид. наук : спеціальність : 12.00.08. Харків, 2004. 430 с.

114. Правова статистика: підруч. для студ. юрид. спец. вищ. навч. закл. / за ред. В. В. Голіни. Харків : Право, 2008. 129 с.

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

116. Про введення в дію рішення Ради національної безпеки і оборони України від 14 травня 2020 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій), з зареєстрованим обліковим записом : Указ Президента України від 14.05.2020 року № 184/2020. URL: https://zakon.rada.gov.ua/laws/show/184/2020#Text (дата звернення: 04.09.2021).

117. Куренкова О. Соціальні мережі-2021: ТікТок старшає, Facebook — переважно жіночий, а стрічку ми гортаємо 400 мільйонів років. URL: https://hromadske.ua/posts/socmerezhi-2021-tiktok-starshaye-facebook-perevazhno-zhinochij-a-strichku-mi-gortayemo-400-miljoniv-rokiv (дата звернення: 04.09.2021).

118. Кримінально процесуальний кодекс : Закон України від 13.04.2012 року № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 04.09.2021).

119. Бурда О. М. Запобігання крадіжкам в мережі роздрібної торгівлі : дис... канд. юрид. наук : спеціальність : 12.00.08. Харків, 2021. 235 с.

120. Кримінологія : підручник / за заг. ред. Л. С. Сміяна, Ю. В. Нікітіна. Київ : Нац. акад. управління, 2010. 496 с.

121. Кримінологія : підруч. для студ. вищ. навч. закл. / за заг. ред. О. М. Джужи. Київ : Юрінком Інтер, 2002. 416 с.

122. Bohdan Holovkin; Oleksii Tavolzhanskyi; Serhii Cherniavskyi. Factors of cybercrime in Ukraine. *Revista Relações Internacionais do Mundo Atual Unicuritiba*. 2023. Vol. 3. p. 464-488.

123. Воронкова В. Г. Глобалізація як процес універсалізації стосунків між державою та ринком. *Гуманітарний вісник Запорізької державної інженерної академії*. 2008. Вип. 35. С. 15-35.

124. Сторожчук В. М. Лібералізація митно-тарифного регулювання зовнішньої торгівлі : дис. … канд. екон. наук : спеціальність : 08.00.02. Київ, 2019. 283 с.

125. Безтелесна Л. І. Соціальний концепт суспільних та економічних процесів національного розвитку : монографія / за наук. ред. Л. І. Безтелесної. Рівне : Волин. обереги, 2015. 184 с.

126. COVID-19: вплив на електронну комерцію. URL: https://yur-gazeta.com/publications/practice/medichne-pravo-farmacevtika/covid19-vpliv-na-elektronnu-komerciyu.html (дата звернення 29.10.2021).

127. COVID-19 нівелює досягнуті успіхи в боротьбі з бідністю в Україні та в усьому світі: доповідь. URL: https://www.ua.undp.org/content/ukraine/uk/home/presscenter/pressreleases/2021/covid-19-reversing-gains-made-in-fighting-poverty-in-ukraine-and.html. (дата звернення 29.10.2021).

128. Валовий внутрішній продукт (ВВП) в Україні 2021. URL: https://index.minfin.com.ua/ua/economy/gdp/ (дата звернення 30.10.2021).

129. Список країн за ВВП (номінал) на душу населення. URL: https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BE%D0%BA_%D0%BA%D1%80%D0%B0%D1%97%D0%BD_%D0%B7%D0%B0_%D0%92%D0%92%D0%9F_(%D0%BD%D0%BE%D0%BC%D1%96%D0%BD%D0%B0%D0%BB)_%D0%BD%D0%B0_%D0%B4%D1%83%D1%88%D1%83_%D0%BD%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F. (дата звернення 02.11.2021).

130. Як пандемія COVID-19 змінила ринок праці в Україні. URL: https://www.ukrinform.ua/rubric-society/3104312-ak-pandemia-covid19-zminila-rinok-praci-v-ukraini.html (дата звернення 29.10.2021).

131. Державна служба статистики України. Зайнятість та безробіття населення в II кварталі 2021 року. URL: www.ukrstat.gov.ua. (дата звернення 29.10.2021).

132. Купівельна спроможність українців впала на 30 %. URL: https://www.unian.ua/economics/finance/kupivelna-spromozhnist-ukrajinciv-vpala-na-30-novini-ukrajina-11517229.html. (дата звернення 29.10.2021).

133. Катинська Л. Р. Питання відповідності Закону України «Про електронну комерцію» європейському законодавству. *Науковий вісник Ужгородського національного університету.* 2015. Вип. 35. Ч. ІІ. Т. 1. С. 165-169.

134. Як уряду України розбудувати державну політику у сфері е-торгівлі. URL: https://www.civic-synergy.org.ua/wp-content/uploads/2018/04/web_E-commerce__civic_synergy_ua_2018.pdf. (дата звернення 03.11.2021).

135. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. канд. юрид. наук : спеціальність : 12.00.09. Донецьк, 2014. 20 с.

136. Булатов А. С. Кримінальне маніпулювання під час шахрайства. *Юридична психологія: науковий журнал*. Київ, 2015. С. 203-213.

137. Чернишов Г. М. Фінансове шахрайство в інвестиційно-будівельній сфері : дис. ... канд. юрид. наук : спеціальність : 12.00.08. Одеса, 2016. 246 с.

138. Загальна теорія держави і права : підручник для студентів юридичних вищих навчальних закладів / за ред. М. В. Цвіка, О. В. Петришина. Харків: Право, 2009. 584 с.

139. Макаренко Л. О. Теоретико-методологічні аспекти пізнання та формування правової культури : дис... канд. юрид. наук : спеціальність : 12.00.01. Київ, 2019. 441 с.

140. Максимов С. І. Правова культура та її роль у реформуванні правової системи. *Вісник Національної юридичної академії України імені Ярослава Мудрого.* 2011. № 8. С. 212-213.

141. Digital trends 2020: Every single stat you need to know about the internet. URL: https://thenextweb.com/growth-quarters/2020/01/30/digital-trends-2020-every-single-stat-you-need-to-know-about-the-internet/ (дата звернення: 03.01.2021).

142. Дзьобань О. П., Соснін О. В. Віртуальна реальність суспільства постмодерну як соціокультурне тло соціалізації «людини інформаційної». *Гуманітарний вісник Запорізької державної інженерної академії: зб. наук. пр*. 2017. Вип. 69 (1). С. 69-76.

143. Гузьман О. А., Ляшенко Н. О. Комп'ютерна залежність підлітків. URL: http://web.kpi.kharkov.ua/sp/guzman-o-a-lyashenko-n-o-komp-yuterna-zalezhnist-pidlitkiv/ (дата звернення: 04.01.2021).

144. Безугла М. В. Формування у студентської молоді духовно-культурних цінностей освіти : автореф. дис. … канд. пед. наук : спеціальність 6 13.00.07. Київ, 2015. 20 с.

145. Афанасенко С. І. Особливості механізму віктимної поведінки жертв шахрайств. *Південноукраїнський правовий часопис.* 2014. № 3. С. 58-61.

146. Валоб'єв А. Ф. Механізм злочину та його зв'язок з концептуальними положеннями криміналістики : монографія. Кривий Ріг : вид. Р. А. Козлов, 2019. 122 с.

147. Дундич Л. В. Поняття і структура механізму злочину. *Форум права*. 2008. № 1. С. 125-129.

148. Мачинська Н. І., Завойська О. Ю. Психологічні механізми учинення злочину. *Науковий вісник Львівського державного університету внутрішніх справ*. 2013. № 1. С. 104-114.

149. Албул С. В., Холотенко А. В. Корислива злочинність: сучасні кримінологічні та кримінально-правові проблеми. *Південноукраїнський правничий часопис.* 2015. № 4. С. 14-16.

150. Газдайка-Василишин І. Б. Корисливий мотив та корислива мета злочинів проти власності. *Науковий вісник Львівського державного університету внутрішніх справ.* 2012. № 2. С. 178-187.

151. Фіалка М. І. Механізм індивідуальної злочинної поведінки, пов'язаної з фальсифікацією документів. *Юридичний науковий електронний журнал*. 2019. № 5. С. 266-270.

152. Прудка Л. М. Психологічні особливості шахрайства в мережі інтернет. Протидія злочинності: проблеми практики та науково-методичне забезпечення. 2018. № 2. С. 30-33.

153. Бандурка О. М., Литвинов О. М. Механізм злочинної поведінки. *Вісник кримінологічної асоціації України*. 2016. № 3 (4). С. 110-119.

154. Лысодед А. В. Об особенностях преступного поведения при мошенничестве. *Вісник Луганського інституту внутрішніх справ МВС*. 2000. № 4. С. 116-126.

155. Туляков В. А. Виктимология: социальные и криминологический проблемы : монография. Одесса : Одесс. нац. юрид. акад., 2000. 480 с.

156. Віктимологія : навч. посібник / за ред. Голіни В. В., Головкіна Б. М. Харків : Право, 2017. 343 с.

157. Кравченко О. В. Психологічні особливості шахрайства : автореферат дис. … канд. психолог. наук : спеціальність : 19.00.06. Харків, 2005. 17 с.

158. Корягіна А. М. Щодо визначення взаємовідносин жертви та злочинця. *Вісник Луганського державного університету внутрішніх справ.* 2010. № 2. С. 287-294.

159. Мішені маніпулятивного впливу. URL: https://oksamyt.org/100420163/ (дата звернення: 02.06.2021).

160. Крива Н. Л. Проблема довіри в сучасній психології. *Теорія і практика сучасної психології.* 2018. № 5. С. 128-132.

161. Чаплак Я. В., Чуйко Г. В. Міжособистісна довіра як передумова партнерських стосунків між людьми. *Psychological journal.* 2020. Вип. 6. С. 29-39.

162. Казміренко Л. І., Кудерміна О. І., Мойсєєва О. Є. Психологія : підручник / за ред. Л. І. Казміренко. Київ : нац. акад. внутр. справ, 2015. 213 с.

163. Психологія : навч. посібник / за ред. Трофімова Ю. Л. Київ: Либідь, 1999. 558 с.

164. Словник української мови: в 11 т. Т. 2. 1971. С. 501.

165. Піраміда потреб Абрагама Маслоу. URL: https://uk.wikipedia.org/wiki/%D0%9F%D1%96%D1%80%D0%B0%D0%BC%D1%96%D0%B4%D0%B0_%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1_%D0%90%D0%B1%D1%80%D0%B0%D0%B3%D0%B0%D0%BC%D0%B0_%D0%9C%D0%B0%D1%81%D0%BB%D0%BE%D1%83 (дата звернення: 02.06.2021).

166. Великий В. М. Сутність і профілактика залежності від азартних ігор. *Медичне право України: правовий статус пацієнта в Україні та його законодавче забезпечення (генезис, розвток, проблеми і перспективи вдосконалення:* матеріали II Всеукр. наук.-практ. конф., 17–18 квітня 2008. Львів, 2008. С. 51-56.

167. Безвідповідальність. URL: http://psychologis.com.ua/bezotvetstvennost.htm (дата звернення: 08.06.2021).

168. Рекуненко Т. О. Методи і прийоми впливу на особистість у правоохоронній діяльності. *Науковий вісник публічного та приватного права*. 2016. Вип. 4. С. 268-271.

169. Гарбан І. О. Вербальні маркери сугерсії в сучасному американському юридичному трилері : дис. … канд. філолог. наук : спеціальність : 10.02.04. Київ - Запоріжжя, 2019. 346 с.

170. Булатов А. С. Кримінальне маніпулювання під час шахрайства. *Юридична психологія*. 2015. № 2. С. 203-211.

171. Прудка Л. М. Психологічні особливості шахрайства в мережі Інтернет. *Південноукраїнський правничий часопис*. 2018. № 2. С. 30-32.

172. Самовпевненість і впевненість у собі. URL: https://molod-sport.khm.gov.ua/%D1%81%D0%B0%D0%BC%D0%BE%D0%B2%D0%BF%D0%B5%D0%B2%D0%BD%D0%B5%D0%BD%D1%96%D1%81%D1%82%D1%8C-%D1%96-%D0%B2%D0%BF%D0%B5%D0%B2%D0%BD%D0%B5%D0%BD%D1%96

%D1%81%D1%82%D1%8C-%D1%83-%D1%81%D0%BE%D0%B1%D1%96/ (дата звернення: 08.06.2021).

173. Попов К. Л. Віктимність в механізмі шахрайства. *Правове регулювання суспільних відносин в умовах демократизації Української держави: матеріали II Міжн. наук.-практ. конф.*, м. Київ, 29 листоп. 2012 р. Київ, 2012. С. 208-210.

174. 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).

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

176. COVID-19 will permanently change e-commerce in Denmark. URL: https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/strategy/e-commerce-covid-19-onepage.pdf (дата звернення: 05.11.2021).

177. E-commerce, trade and the COVID-19: pandemic information note. URL:https://www.wto.org/english/tratop_e/covid19_e/ecommerce_report_e.pdf (дата звернення: 05.11.2021).

178. Конференция Организации Объединенных Наций по торговле и развитию (ЮНКТАД). URL: https://www.ungeneva.org/ru/about/organizations/unctad (дата звернення: 09.11.2021).

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

180. Ecommerce Fraud + 11 Fraud Prevention Strategies. URL: https://www.bigcommerce.com/blog/ecommerce-fraud/#what-is-ecommerce-fraud (дата звернення: 11.11.2021).

181. 2021 Global Payment Risk Mitigation Report. Worldpay from FIS. URL: https://offers.worldpayglobal.com/global-payment-risk.html (дата звернення: 14.11.2021).

182. LexisNexis Risk Solutions Group. URL: https://risk.lexisnexis.com/ (дата звернення: 14.11.2021).

183. E-Commerce and Consumer Protection in India. URL: https://link.springer.com/article/10.1007/s10551-021-04884-3 (дата звернення: 16.11.2021).

184. 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).

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

186. Краткое изложение Закона США о безопасности в Интернете. 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).

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

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

189. China’s new E-commerce Law: tools in the fight against IP rights infringement. URL: https://www.worldtrademarkreview.com/anti-counterfeiting/chinas-new-e-commerce-law-tools-fight-against-ip-rights-infringement (дата звернення: 25.11.2021).

190. New Chinese Cybersecurity and Data Privacy Requirements. URL: https://www.jonesday.com/en/insights/2020/12/new-chinese-cybersecurity-and-data-privacy-requirements (дата звернення: 25.11.2021).

191. Cyber Security and Technology Crime | Hong Kong Police Force. URL: https://www.police.gov.hk/ppp_en/04_crime_matters/tcd/index.html (дата звернення: 26.11.2021).

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

193. Що таке служба підтвердження адрес (avs)? – визначення з техопедії. URL: https://uk.theastrologypage.com/address-verification-service (дата звернення: 28.11.2021).

194. Центр Google Поиска. Как защитить сайт с помощью HTTPS. URL:https://developers.google.com/search/docs/advanced/security/https?hl=ru (дата звернення: 28.11.2021).

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

196. Kount. URL: https://kount.com/ (дата звернення: 30.11.2021).

197. Велика українська юридична енциклопедія : у 20 т. Кримінологія. Кримінально-виконавче право / за ред. В. І. Шакун, В. І. Тимошенко. Харків : Право, 2009. Т. 18. 544 с.

198. Про затвердження Національної економічної стратегії на період до 2030 року : Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennya-nacionalnoyi-eko-a179 (дата звернення: 07.04.2021 року).

199. Фаріон М., Бута М. Подолання бідності: що важливіше, темп зростання чи якість інструменів. *Галицкий экономический журнал.* 2020. Т. 63. Вип. 2. С. 84-95.

200. Global Compact Network Ukraine. Цілі сталого розвитку. URL: https://globalcompact.org.ua/pro-nas/tsili-stijkogo-rozvytku/ (дата звернення: 07.01.2022 року).

201. Про схвалення Стратегії подолання бідності : Розпорядженя КМУ від 16.03.2016 р. № 161-р. URL: https://www.kmu.gov.ua/npas/248898080 (дата звернення: 09.01.2022 року).

202. Мінсоцполітики. Рівень життя та бідності населення. URL: https://pon.org.ua/novyny/9097-riven-zhyttia-naselennia-ta-riven-bidnosti-informuie-minsocpolityky.html (дата звернення: 08.01.2022 року).

203. Слюсар С. Т. Аналіз рівня безробіття в Україні: проблеми і шляхи його подолання. *Економіка АПК*. 2018. № 5. С. 85-92.

204. Про зайнятість населення : Закону України від 05.07.2012 року № 5067-VI. URL: https://zakon.rada.gov.ua/laws/show/5067-17#n138 (дата звернення: 09.01.2022 року).

205. Про затвердження Основних напрямів реалізації державної політики у сфері зайнятості населення та стимулювання створення нових робочих місць на період до 2022 року : розпорядження Кабінету Міністрів України від 24.12.2019 р. № 1396-р. URL: https://zakon.rada.gov.ua/laws/show/1396-2019-%D1%80#Text (дата звернення: 12.01.2022 року).

206. Герасіна Л. М., Панов М. І., Требін М. П. Деформації правосвідомості та правової культури сучасного українського суспільства. Правосвідомість і правова культура як базові чинники державотворчого процесу в Україні : монографія / за ред. Л. М. Герасіна, О. Г. Данильяна, О. П. Дзьобань та ін. Харків, 2009. 352 с.

207. Клімова Г. П. Основні шляхи формування правосвідомості і правової культури українських громадян в умовах розбудови правової держави. Правосвідомість і правова культура як базові чинники державотворчого процесу в Україні : монографія / за ред. Л. М. Герасіна, О. Г. Данильяна, О. П. Дзьобань та ін. Харків, 2009. 352 с.

208. Головкін Б. М. Теперішнє і майбутнє кримінології. *Проблеми законності.* 2020. Вип. 149. С. 168-184.

209. Понятийный аппарат современной криминологии. Терминологический словарь. / под ред. А. Г. Кальман, И. А. Христич. Харков : Гимназия, 2005. 273 с.

210. Запобігання злочинності (теорія і практика) : навч. посібник / за ред. Голіна В. В. Харьков : Нац. юрид. акад. України, 2011. 120 с.

211. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX. URL : https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 21.01.2022 року).

212. Про захист прав споживачів : Закон України від 12.05.1991 № 1023-XII. URL : https://zakon.rada.gov.ua/laws/show/1023-12 (дата звернення: 21.01.2022 року).

213. Про електронні комунікації : Закон України від 01.01.2022 р. № 2240-IX. URL : https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 21.01.2022 року).

214. Закон про електронні комунікації: універсальний доступ, субсидії на Інтернет, захист персональних даних та ризик шатдаунів в зоні АТО. Лабораторія цифрової безпеки. URL : https://dslua.org/publications/zakon-pro-elektronni-komunikatsii-universalnyy-dostup-subsydii-na-internet-zakhyst-personalnykh-danykh-ta-ryzyk-shatdauniv-v-zoni-ato/ (дата звернення: 21.01.2022 року).

215. Центр демократії та верховенства права. Як захиститись від спаму? URL : https://cedem.org.ua/consultations/zahystytysya-vid-spamu/ (дата звернення: 21.01.2022 року).

216. Лефтеров Л. В. Загальносоціальні заходи запобігання шахрайству, що вчиняється шляхом використання засобів електронних комунікацій. *Lex Portus*. № 1 (15), 2019. С. 89-101.

217. ПриватБанк. Безпека. URL : https://privatbank.ua/ (дата звернення: 21.01.2022 року).

218. Закалюк А.П. Курс сучасної української кримінології: теорія і практика : у 3 кн. Київ : Ін Юре, 2007. Кн. 1: Теоретичні засади та історія української кримінологічної науки. 2007. 424 с.

219. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 21.02.2022 року).

220. Про засади внутрішньої і зовнішньої політики : Закон України від 01.07.2010 р. № 2469-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 21.02.2022 року).

221. Про Кабінет міністрів України : Закон України від 04.02.2009 р. № 922-VI. URL : https://zakon.rada.gov.ua/laws/show/794-18#Text (дата звернення: 11.03.2022 року).

222. Про центральні органи виконавчої влади : Закон України від 12.12.2007 р. № 1185. URL : https://zakon.rada.gov.ua/laws/show/3166-17#Text (дата звернення: 11.03.2022 року).

223. Питання Міністерства економіки : Постанова КМУ від 20.08.2014 р. № 459. URL : https://ips.ligazakon.net/document/KP140459?an=1634 (дата звернення: 12.03.2022 року).

224. Питання Міністерства цифрової трансформації : Постанова КМУ від 18.09.2019 р. № 856. «URL : https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text (дата звернення: 14.03.2022 року).

225. Про місцеві державні адміністрації : Закон України від 09.04.1999 р. № 586-XIV. URL : https://zakon.rada.gov.ua/laws/show/586-14#Text (дата звернення: 14.03.2022 року).

226. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.2006 р. № 3475-IV. URL : https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 15.03.2022 року).

227. Про Державний центр кіберзахисту та протидії кіберзагрозам CERT-UA. URL : https://ips.ligazakon.net/document/TO001440 (дата звернення: 15.03.2022 року).

228. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 14.05.2021 р. № 447/2021. URL : https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 15.03.2022 року).

229. Про національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 16.03.2022 року).

230. Офіційний сайт Департаменту кіберполіції Національної поліції України. URL : https://cyberpolice.gov.ua (дата звернення: 16.03.2022 року).

231. Аваков А. Б. Кіберполіція (крок реформі). URL : https://www.facebook.com/arsen.avakov.1/posts/916452195111554 (дата звернення: 16.03.2022 року).

232. Небеська М. С., Салман А. С. Органи внутрішніх справ як суб'єкт запобігання злочинності. *Південноукраїнський правничий часопис*. 2015. № 2. С. 34-36.

233. Національний Банк України. Стартує інформаційна кампанія Національного банку з платіжної безпеки #ШахрайГудбай. URL : https://bank.gov.ua/ua/news/all/startuye-informatsiyna-kampaniya-natsionalnogo-banku-z-platijnoyi-bezpeki-shahraygudbay (дата звернення: 17.03.2022 року).

234. Загальна Декларація прав людини : прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 19.03.2022 року).

235. Мокряк М. О. Превентивна функціональність засобів масової інформації як теоретична конструкція та практична діяльність. *Науковий вісник Міжнародного гуманітарного університету*. 2017. № 30. Т. 2. С. 69-71.

236. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького.* Серія : Право. 2018. № 6. С. 154-163.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1) Коновалова І. О. Шахрайство і діджиталізація: історико-правовий аналіз. *Право і суспільство.* 2021. Вип. 3. С. 105-113.

2) Коновалова І. О. Жертва в електронному торговельно-комерційному шахрайстві. *Науковий вісник Ужгородського національного університету.* Серія : Право. Ужгород, 2021. № 65. С. 266-271.

3) Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. *Науковий вісник Ужгородського національного університету.* Серія : Право. Ужгород, 2021. № 68 (6). С. 220-225.

4) Коновалова І. О. Кримінологічна характеристика сучасного стану шахрайства у сфері електронної торгівлі. *Recht der Osteuropäischen Staaten.* 2022. № 1. С. 11-18.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

5) Коновалова І. О. До питання шахрайств у сфері електронної торгівлі. *Протидія організованій злочинності і корупції : матеріали XIX Всеукр. наук. конф. з кримінології для студентів, аспірантів та молодих вчених* (м. Харків, 2 груд. 2019 р.). Харків : Право, 2019. С. 69-71.

6) Konovalova Ilona. Modern forms of fraud. *Сучасне суспільство і наука: актуальні дослідження молодих науковців : матеріали Всеукр. наук.-практ. інтернет-конф. іноземними мовами*., (Харків, 29 травня 2020 р.). Харків : НЮУ ім. Ярослава Мудрого, 2020. С. 56-58.

7) Коновалова І. О., Пивоваров В. В. Шахрайство в умовах діджиталізації суспільства. *Діджиталізація і безпека : матеріали Міжнар. наук.-практ. конф*., (Харків, 19 листоп. 2020 р.). Харків : Право, 2020. С. 167-173.

8) Коновалова І. О. Щодо жертви електронного комерційного шахрайства. *Протидія злочинності і корупції : міжнародні стандарти та досвід України: зб. тез Міжнар. конф.* (м. Харків, 22 вересня 2021 р.). Харків: Юрайт, 2021. С. 156-160.

9) Коновалова І. О. Загальносоціальні заходи запобігання електронному торгівельному шахрайству. *Наукові читання, присвячені пам'яті професора Т. А. Денисової : зб. матеріалів* (м. Запоріжжя, 10 березня 2022 р.). Запоріжжя : КПУ, 2022. С. 442-445.

Додаток Б

СПЕЦІАЛІЗОВАНА АНКЕТА
ДЛЯ ВИБІРКОВОГО УЗАГАЛЬНЕННЯ МАТЕРІАЛІВ
КРИМІНАЛЬНИХ
ПРОВАДЖЕННЬ ЩОДО ШАХРАЙСТВА У СФЕРІ ЕЛЕКТРОННОЇ
ТОРГІВЛІ

Кримінальне провадження № _____, суд _____,
від _____.

Відомості про злочин

1. Кваліфікація діяння:_____
2. Вид електронного шахрайства: _____
3. Площадка (сайт) вчинення кримінального правопорушення: _____
4. Спосіб вчинення злочину: _____
5. Предмет злочину (вид товару): _____
6. Форма співучасті: _____

Потерпілий

1. Фізична особа-підприємець: _____
2. Юридична особа: _____
3. Відомості щодо цивільного позову (так \ ні; сума) : _____
4. Відомості, щодо відшкодування завданої шкоди : _____

Вид і розмір призначеного покарання

_____.

Додаток В

Зведені дані інтерактивного опитування співробітників правоохоронних органів (2022 р.) щодо шахрайств у сфері електронної торгівлі

1. Місце роботи:

1) Національна поліція України – 24 %;
2) Прокуратура – 24 %;
3) Служба безпеки України – 0 %;
4) Адвокатура – 16 %;
5) Суд – 16 %;
6) Інше: 20 %.

2. Ваш вік:

1) до 30 років – 50 %;
2) 30 - 45 років - 40 %;
3) 45 років і старше – 10 %.

3. Стаж роботи:

1) до 3-х років - 24 %;
2) від 3-х до 5-ти років – 22 %;
3) від 5-ти до 10-ти років – 22 %;
4) більше 10-ти років – 32 %.

4. Чи доводилося Вам виявляти, розслідувати, здійснювати процесуальне керівництво, підтримувати державне обвинувачення, проводити судовий розгляд щодо шахрайств у сфері електронної торгівлі?

1) Так – 52 %;
2) Ні – 48 %.

5. Оцініть рівень латентності шахрайства у сфері електронної торгівлі:

1) на один зареєстрований злочин припадає десять і більше незареєстрованих – 48 %;
2) на один зареєстрований злочин припадає чотири та більше незареєстрованих – 26 %;
3) на один зареєстрований злочин припадає від двох до трьох незареєстрованих - 18 %;
4) на один зареєстрований злочин припадає один незареєстрований – 0 %;
5) не можу відповісти – 8 %

6. Вкажіть, чому не всі шахрайства у сфері електронної торгівлі виявляються і реєструються:

1) не має реальних заявників (потерпілої особи) – 17,6 %;
2) недосконаліть законодавства – 18,7 %;
3) високий рівень корумпованості органів державної влади, правоохоронних органів, контролюючих суб'єктів та органів місцевого самоврядування – 5,4 %;
4) недостатня кваліфікація працівників правоохоронних органів – 17,6 %;
5) складність розслідування та отримання доказової інформації – 40,7 %;

7. Стать особи, яка вчинила кримінальне правопорушення:

1) чоловіча – 93,3 %;
2) жіноча – 6,7 %.

8. Вік особи, яка вчинила кримінальне правопорушення:

1) від 18 до 25 років – 24,4 %;
2) від 25 до 35 років – 51,1 %;
3) від 35 до 45 років – 20 %;
4) понад 45 років – 4,6 %.

9. Сімейний стан особи, яка вчинила кримінальне правопорушення:

1) не одружений / не заміжня – 56,8 %;
2) одружений / заміжня – 20,5 %;
3) розлучений / розлучена – 0 %;
4) вдівець / вдова – 0 %;
5) перебувають у фактичних шлюбних відносинах – 22,7 %.

10. Освіта особи, яка вчинила кримінальне правопорушення:

1) початкова загальна освіта – 2,3 %;
2) базова загальна середня освіта – 9,3 %;
3) повна загальна середня освіта – 27,9 %;
4) професійно-технічна освіта – 23,3 %;
5) базова вища освіта – 11,6 %;
6) повна вища освіта – 25,6 %.

11. Спеціальність особи, яка вчинила кримінальне правопорушення:

1) економічна – 14,3 %;
2) юридична – 0 %;
3) технічна (зокрема, комп'ютерні технології) – 61,9 %;
4) психологічна – 0 %;
5) інше: 23,8 %.

12. Судимість особи, яка вчинила кримінальне правопорушення:

1) не судима раніше – 63,6 %;
2) знята або погашена судимість – 18,2 %;
3) відбуває покарання – 18,2 %.

13. Вкажіть основні мотиви вчинення шахрайства у сфері електронної торгівлі:

1) крайня нужда в елементарних матеріальних благах – 3 %;
2) бажання мати додаткові кошти на власні потреби та потреби сім'ї – 8 %;

3) бажання незаконного збагачення у великих та особливо великих розмірах – 28 %;
4) бажання покращити матеріальне становище, підняти рівень побутового комфорту і створити нові споживацькі можливості (відпочинок, розваги, престижний одяг, інші витрати) – 50 %;
5) бажання набути високого соціального становища внаслідок постійного джерела незаконних доходів – 8 %;
6) необхідність погасити кредити та боргові зобов'язання – 0 %;
7) інше: безкарність - 6 %.

14. Просимо Вас висловити власну думку щодо ефективних шляхів запобігання шахрайству у сфері електронної торгівлі:

1) Превентивна та просвітницька діяльності серед населення;
2) Прив'язування мобільних номерів до паспорта;
3) Розширення можливостей кіберполіції;
4) Налагодження співпраці зі спеціалістами у сфері кібербезпеки (можливість призначати дослідження у спеціалістів про інформацію дій осіб, які вчинили кримінальне правопорушення у сфері електронної торгівлі та надання останніми висновку, за правдивість та достовірність якого спеціаліст несе кримінальну відповідальність (як висновок експерта));
5) Ведення електронної торгівлі тільки гарантованими учасниками ринку, які мають страховий пакет на випадок ризиків;
6) Підвищення кваліфікації працівників поліції в цій сфері, заручення спеціалістів цієї галузі на контрактній основі;
7) Посилення відповідальності за вчинення кримінального правопорушення;
8) Спрощення процесуальної процедури розслідування кримінального правопорушення;

9) Регламентування роботи онлайн-майданчиків та сервісів з оголошеннями;
10) Відповідальність власників ресурсів за розміщення неперевірених оголошень та випадків шахрайства на конкретному сервісі;
11) Авторизація на майданчиках через дію або ЕЦП.

15. Які напрями роботи правоохоронних органів слід посилити для ефективнішого запобігання шахрайству у сфері електронної торгівлі:

1) Кібербезпека;
2) Процесуальна складова - зменшити залежність органів від прокуратури та надати більше самостійності та повноважень органам безпеки;
3) Спрощення обміну інформацією між операторами телекомунікаційних мереж та правоохоронними органами;
4) Підвищити кваліфікацію та забезпечення кіберполіції;
5) Надати прямий доступ до всіх державних реєстрів;
6) Випередження виникнення криміногенних явищ і процесів, що сприяють вчиненню шахрайства;
7) Превентивна діяльність та робота з населенням для підвищення рівня правової обізнаності.

Додаток Г

Зведені дані інтерактивного опитування потенційних жертв шахрайства у сфері електронної торгівлі

1. **Ваш вік:**
   1) до 18 років – 1,4 %;
   2) 18 - 30 років – 43,9 %;
   3) 31 - 40 років – 20,7 %;
   4) 41- 50 років – 14 %;
   5) 51 - 65 років – 16,5 %;
   6) 66 років і старше – 3,5 %.
2. **Чим Ви займаєтесь?**
   1) Навчаюсь в школі – 10,8 %;
   2) Навчаюсь в ВНЗ (студент) – 16,4 %;
   3) Службовець – 20,6 %;
   4) Підприємець – 16,4 %;
   5) Найманий працівник - 32,8 %;
   6) Пенсіонер – 3 %;
   7) Інше (вкажіть, що саме _____)
3. **Чи були Ви або Ваші близькі, друзі жертвою шахрайства у сфері електронної торгівлі?**
   1) Так – 72,7 %;
   2) Ні – 27,3 %.
4. **Який розмір шкоди було завдано Вам або Вашим близьким, друзям шахрайством у сфері електронної торгівлі?**
   1) До 500 грн – 31,5 %;
   2) Від 500 до 1000 грн – 22,5 %;
   3) Від 1 000 грн до 5 000 грн – 11,3 %;
   4) Від 5 000 грн до 10 000 грн – 5 %;
   5) Від 10 000 грн до 100 000 грн – 31,5 %;

6) Понад 100 000 грн – 5 %.

5. Наскільки поширеними, на Ваш погляд, є шахрайські порушення закону у сфері електронної торгівлі в Україні (визначте за шкалою від 0 до 10, де 0 – майже відсутні, 10 – надзвичайно поширені) ?

1) – 3 (**1,1 %**);
2) - 3 (**1,1 %**);
3) – 5 (**1,8 %**);
4) – 13 (**12,3 %**);
5) – 35 (**12,3 %**);
6) – 34 (**11,9 %**);
7) – 46 (**16,1 %**);
8) – 57 (**20 %**);
9) – 25 (**8,8 %**);
10) - 64 (**22,5 %**);

6. Які види злочинів найбільш поширені у сфері електронної торгівлі? (оберіть не більше трьох):

1) Незаконні дії з електронними грошима – 114 (**17,2 %);**
2) Викрадення персональних даних – 145 (**21,8 %**);
3) Підробка платіжних карток – 68 (**10,3 %**);
4) Збут наркотичних речовин – 59 (**8,9 %**);
5) Легалізація (відмивання) доходів, одержаних злочинним шляхом – 46 (**6,9 %**);
6) Шахрайство в інтернет-торгівлі – 233 (**34,9 %**);
7) Інше (вкажіть, що саме _____)

7. Найбільш приваблива для шахраїв:

1) кредитно-банківська сфера – 51,7 %;
2) галузь підприємництва (у тому числі й електронна комерція) – 19,6 %;
3) зовнішньоекономічна галузь – 0,7 %;
4) сфера послуг населенню – 15,7 %;

5) ігорний бізнес – 7,3 %;
6) ринок нерухомості – 3,5 %;
7) ринок цінних паперів – 0 %;
8) страхування – 0,7 %.

8. За вашим досвідом, предмети шахрайства в електронній торгівлі – це (вкажіть три найбільш популярних):

1) валютні кошти – 109 (**14,4 %**);
2) одяг, взуття та модні аксесуари - 144 (**19,1 %**);
3) побутова техніка та електроніка – 85 (**11,3 %**);
4) мобільні телефони, смартфони, планшети – 138 (**18,4 %**);
5) товари для дому та саду - 26 (**3,5 %**);
6) предмети гігієни – 4 (**0,5 %**);
7) косметика і парфумерія – 28 (**3,7 %**);
8) елітний алкоголь – 27 (**3,6 %**);
9) тютюнові вироби, приладдя для паління – 13 (**1,7 %**);
10) товари медичного призначення – 46 (**6,1 %**);
11) продукти харчування – 9 (**1,2 %**);
12) ювелірні вироби та коштовності – 37 (**4,8 %**);
13) предмети колекціонування – 28 (**3,7 %**);
14) товари, що були у використанні (всілякі вживані речі) – 58 (**7,7 %**);
15) інші матеріальні цінності (вкажіть, які _____): криптовалюта – 1 (**0,1 %**); надання онлайн-послуг – 1 (**0,1 %**); тренінги – 1 (**0,1 %**).

9. На Вашу думку, шахрайство у сфері електронної торгівлі найчастіше вчиняється шляхом (вкажіть не більше двох варіантів):

1) фішингу – 167 (**27,6 %**);
2) шахрайства з авансовим платежем/передплатою – 166 (**27,4 %**);
3) шахрайства з підробкою платіжних квитанцій – 20 (**3,3 %**);
4) крадіжок персональних даних, злому облікових записів – 84 (**13,9 %**);

5) шахрайства з доставкою – 33 (**5,4 %**);
6) шахрайства з платіжними картами – 71 (**11,7 %**);
7) шахрайства при користуванні мобільними телефонами, зокрема додатками Google Pay, ApplePay, PayPass – 34 (**5,6 %**);
8) шахрайських платіжних систем – 31 (**5,1 %**).

10. На Вашу думку, які риси жертви намагаються використовувати шахраї:

1) жадібність -11,5 %;
2) азарт – 2,8 %;
3) віра у щасливий випадок, везіння, «фарт» - 13,2 %;
4) неуважність – 12,2 %;
5) довірливість – 54,7 %;
6) навіюваність – 1,7 %;
7) безвідповідальність – 2,1 %;
8) самовпевненість - 2,1 %;
9) інше (вкажіть, що саме _____)

11. Шахрайство у сфері електронної торгівлі потребує складної підготовки до вчинення злочину, використання службового становища чи корупційних зв'язків?

1) Так – 30,2 %;
2) Ні – 38,2 %;
3) Важко відповісти – 31,6 %.

12. Ваша думка: що спонукає шахраїв на злочини у сфері електронної торгівлі? (вкажіть не більше трьох)

1) Висока прибутковість таких злочинів – 143 (**20,2 %**);
2) Недосконалість законодавства у сфері електронної торгівлі – 127 (**18 %**);
3) Недосконалість державного контролю за електронною торгівлею – 136 (**19,5 %**);
4) Недосконала робота правоохоронних органів - 114 (**16 %**);

5) Відсутність ефективної взаємодії державних органів між собою – 39 (**5,5 %**);
6) Поведінка жертви (недбалість, необізнаність, зайва довірливість тощо) – 148 (**20,8 %**).

Додаток Д

Акти впровадження

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ГОЛОВНЕ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В ХАРКІВСЬКІЙ ОБЛАСТІ
ХАРКІВСЬКЕ РАЙОННЕ УПРАВЛІННЯ ПОЛІЦІЇ № 1 ВІДДІЛ ПОЛІЦІЇ № 2
Пров. Балашовський, 12, м. Харків, 61001
Тел. (057)737-23-46
e-mail: kh.ro62@police.gov.ua

25.05. 2023 № 4407/119/62/04/11-23

Ректору
Національного юридичного
університету імені Ярослава Мудрого
Анатолію Гетьману
вул. Пушкінська, 77 м. Харків, 61024

АКТ
про впровадження наукових результатів дисертаційного дослідження
у практичну діяльність органів поліції

Розглянувши аналітичну довідку від 19.05.2023 року № 243-0806-632 за матеріалами дисертаційного дослідження аспірантки кафедри кримінально-правової політики Національного юридичного університету імені Ярослава Мудрого І. Коновалової за темою «Запобігання шахрайству у сфері електронної торгівлі» (науковий керівник – кандидат юридичних наук, доцент – Сметаніна Н. В.), робимо висновок про важливість викладеної інформації щодо способів, предметів протиправних посягань, розміру завданої шкоди, показників латентності, відомостей про контингент правопорушників, причини та умови вчинення шахрайств у сферы електронної торгівлі, міжнародний досвід їх запобігання, а також, визначені пріоритети і заходи превентивної діяльності служб і підрозділів Національної поліції України.

Викладена в аналітичній довідці інформація може бути використана в роботі аналітичних, оперативних, превентивних і слідчих підрозділів Національної поліції України в Харківській області, при плануванні та проведенні оперативно-розшукових, оперативно-профілактичних, превентивних заходів, просвітницької роботи із особовим складом та роз'яснювальної роботи серед електронних споживачів та підприємців.

Начальник ВП № 2 ХРУП № 1
ГУНП в Харківській області
полковник поліції **АНДРІЙ ШЕВЧЕНКО**