УДК 004.946.5.056:339.9
DOI https://doi.org/10.32782/TNU-2707-0581/2025.5/24

Давидюк В. М.
Вищий навчальний приватний заклад «Дніпровський гуманітарний університет»

КІБЕРЗЛОЧИННІСТЬ У ЗОВНІШНЬОЕКОНОМІЧНІЙ ДІЯЛЬНОСТІ: ВИКЛИКИ ТА РИЗИКИ

У цій статті здійснено дослідження проблеми кіберзлочинності у сфері зовнішньоекономічної діяльності (далі – ЗЕД) в умовах глобальної цифровізації.

Підкреслено, що зростаюча залежність міжнародної торгівлі від інформаційно-комунікаційних технологій супроводжується стрімким зростанням кіберризиків, що створюють додаткові загрози для економічної безпеки суб'єктів господарювання та світової спільноти.

Визначено основні форми кіберзлочинів, характерних для учасників ЗЕД : фішинг, соціальна інженерія, несанкціонований доступ до корпоративних баз даних, поширення шкідливого програмного забезпечення, шахрайство з використанням корпоративної електронної пошти (так зване Business Email Compromise). З'ясовано, що наслідками таких діянь є значні фінансові збитки, репутаційні втрати, порушення строків виконання контрактів та виникнення міжнародних господарських спорів.

Наведено статистичні дані щодо динаміки кіберзлочинів, які свідчать про щорічне зростання кількості атак та ускладнення їхніх механізмів. Особливу увагу приділено аналізу реальних випадків шахрайства, зафіксованих в Україні, що підтверджують актуальність обраної проблематики та необхідність підвищення рівня кіберзахисту бізнесу.

Визначено, що нормативно-правові механізми реагування на кіберзлочинність у ЗЕД поки не повною мірою відповідають сучасним технологічним викликам. Обґрунтовано доцільність гармонізації українського законодавства з міжнародними стандартами, зокрема положеннями Конвенції про кіберзлочинність.

Акцентовано увагу на потребі розбудови ефективної системи взаємодії між державними органами, правоохоронними структурами, приватним сектором та ІТ-фахівцями для забезпечення комплексної протидії кіберзлочинності. Деталізовано, що підвищення рівня правової обізнаності учасників ЗЕД, впровадження сучасних цифрових засобів захисту та посилення міжнародного співробітництва є ключовими умовами мінімізації ризиків у кіберпросторі.

Ключові слова: *кіберзахист, кіберзлочинність, зовнішньоекономічна діяльність, фішинг, соціальна інженерія, комерційна таємниця, промислове шпигунство.*

Постановка проблеми. В сучасних умовах розвитку цивілізації людство все активніше використовує інформаційні технології у своєму житті і сфера зовнішньоекономічної діяльності не є виключенням. Беззаперечно, стрімкий процес цифровізації здійснив колосальний вплив на міжнародну торгівлю. Разом з тим, остання стає все більш залежною від інформаційно-комунікаційних систем та технологій, що в свою чергу породжує протилежний аспект, – додаткові можливості не тільки для бізнесу, а й для протиправної діяльності.

Незважаючи на те, що бізнес намагається активно реагувати на загрози завдяки перш за все залученню айті-фахівців, державний механізм і нормативне регулювання таких процесів в свою чергу, як правило, реагує з певним запізненням від реальних суспільних процесів. Враховуючи стрімку змінюваність технологій та цифрових тенденцій у сфері діяльності суб'єктів господарювання зазначимо, що проблема кіберзлочинності у ЗЕД залишається не в повній мірі дослідженою. Здійснений нами подальший аналіз піднятої тематики має на меті виявити основні ризики і ступінь залученості державних та приватних структур у забезпеченні протидії кіберзлочинності у сфері ЗЕД.

Аналіз останніх досліджень і публікацій. Дослідженню проблеми боротьби з кіберзлочинністю приділяли увагу такі вітчизняні вчені як О.М. Петровський, С.Ю. Лівчук, М.В. Журавель, Т.О. Чернадчук та ін. Дослідженню забезпечення кібербезпеки та аналізу європейського досвіду приділено увагу в працях Я.С. Мануілова, В.В. Маркова, Ю.І. Хлапоніна, С.В. Кондакова, Є.Є.Шабала, Л.П. Юрчук та ін. Вразливі питання у кібербезпеці досліджував науковець Д. Нікулеско та інші, а сучасні тенденції організованої кіберзлочинності – М.В. Гуцалюк та інші вчені.

Проте, проблема дослідження кіберзлочинності крізь призму ЗЕД залишилася комплексно не розглянутою.

Постановка завдання. Метою цього дослідження є визначення сучасних викликів та ризиків стосовно існування кіберзлочинності у зовнішньоекономічній діяльності. Окреслення проблем, які у короткостроковій та середньостроковій перспективах підлягатимуть вирішенню на державному та міжнародному рівнях.

Виклад основного матеріалу дослідження. Цифрові технології характеризуються низкою переваг. Для бізнесу – це, перш за все, швидка комунікація, оперативність здійснення розрахунків, оптимізація логістичних ланцюгів, автоматизація облікових процесів тощо. Поряд з цим, одним із ключових викликів у безпековій сфері інтернет-простору є соціальна інженерія, злам корпоративних систем і баз даних, розповсюдження шкідливого програмного забезпечення на пристроях суб'єкта господарювання, фішинг та маніпуляції з міжнародними платежами.

Відповідно до офіційної статистики, у період з 2022 року по 2024 рік Україна увійшла в першу трійку держав, які зазнавали найбільшої кількості кібератак [1]. Повномасштабне вторгнення послугувало лише каталізатором таких процесів. Так, починаючи з 24 лютого 2022 року російські хакери стабільно заподіюють шкоду веб-сайтам державної влади України та великому бізнесу. Нагадаємо, що у 2023 році від дій росіян постраждала компанія «Київстар», а у 2024, – дата-центр «Парковий», «Нафтогаз», «Укрзалізниця», «Укрпошта», система «Шлях» [2]. Окреслимо, що перелічені випадки не є вичерпними. За даними швейцарського Cyber Peace Institute, з січня 2022 року по грудень 2023-го було здійснено 3255 кібератак, з яких – 574 на Україну [2]. То ж дана проблема є вельми актуальною на даний час.

В той же момент, у світі зростають випадки шахрайства з використанням електронної пошти бізнесу, що охоплює як малі місцеві підприємства, так і великі корпорації.

Шахрайство з використанням електронної пошти бізнесу полягає в отриманні зловмисниками доступу до корпоративної електронної пошти та здійсненні імітації офіційного листування з метою введення в оману контрагента та схиляння останнього до здійснення неправомірного переказу коштів чи надання конфіденційних даних. Зловмисники зламують корпоративну пошту або створюють схожу адресу електронної пошти підприємства та надсилають контрагенту листа із проханням «терміново провести платіж з оновленими банківськими реквізитами».

Варто зазначити, що жертвою таких правопорушників стають переважно компанії, яким властиво мати значний обіг електронного листування або організації з розгалуженою структурою (з численними філіями, департаментами, дочірніми компаніями), де можна втратити дійсну документацію серед численних листів. Навантажені великою кількістю задач та документації, бухгалтер або менеджер суб'єкта господарювання нічого не підозрюють і здійснюють перерахування коштів на рахунок, що контролюють злочинці. Коли шахрайство розкривається – гроші вже переказані за кордон, а відстежити винних складно. Як наслідок, юридичні особи несуть фінансові збитки, репутаційні втрати, порушуються строки виконання контрактів, що тягне за собою можливе виникнення юридичних спорів.

Закордонні спеціалісти навіть мають статистичні дані з піднятої нами проблематики. До прикладу, у період з грудня 2021 року по грудень 2022 року зафіксовано збільшення на 17 % ідентифікованих глобальних фінансових втрат, пов'язаних із цим видом шахрайства [3]. У 2022 році Центр скарг на інтернет-злочини повідомив про зростання кількості випадків такого виду шахрайства, зокрема в секторі нерухомості, а також інцидентів, коли кошти перераховувалися безпосередньо на криптовалютні біржі або на фінансові установи, що обслуговують кастодіальні рахунки криптовалютних платформ [3]. Випадки описаного вище нами виду шахрайства зафіксовано в усіх штатах Сполучених Штатів Америки (далі – США) та 177 країнах світу, причому понад 140 країн отримували шахрайські грошові перекази [3]. Згідно з фінансовими даними, поданими до Центру скарг на інтернет-злочини в США за 2022 рік, банки, розташовані в Гонконгу та Китаї, були основними міжнародними пунктами призначення привласнених коштів [3]. На другому місці опинилося Сполучене Королівство Великої Британії та Північної Ірландії, яке часто виступає посередницькою ланкою у русі коштів, а також Мексика та Сінгапур [3].

Беззаперечно можна стверджувати, що з кожним роком кількість таких кібератак збільшується та зростає їхня складність. Зокрема, нещодавно в Україні мережу інтернет сколихнула новина про українську підприємицю, яка мала відкриті бізнес-рахунки в Акціонерному Товаристві «УНІВЕРСАЛ БАНК» (Монобанк). Так, підприємиця стала жертвою шахраїв, які діяли в месенджері

Телеграм під виглядом несправжнього бота-помічника Монобанку. Як наслідок, український суб'єкт господарювання був впевнений що спілкується з реальним чат-ботом Монобанку та за 24 години спілкування з шахраями жінка безповоротно втратила 6 мільйонів гривень зі свого бізнес-рахунку [4].

Таким чином, можемо прийти до висновку, що у своїй сукупності кіберзлочини у сфері ЗЕД можуть призвести до значних фінансових втрат потерпілої юридичної особи, негативних репутаційних ризиків для неї, що знайде свій прояв у зниженні довіри партнерів та покупців до продукту або послуги та (або) відобразиться у невиконанні умов договірних зобов'язань. В цьому контексті важливо зазначити, що компанії, що перебувають у зоні найбільшого ризику це ті, що мають значну кількість контрагентів, партнерів, великий документообіг та складні ланцюги постачання.

Також важливо зазначити, що 5 жовтня 2017 року Верховною Радою України було прийнято Закон України «Про основні засади забезпечення кібербезпеки України» [5]. Завдяки згаданому нами закону, українське законодавство поповнилося чіткою і зрозумілою термінологією, що знаходиться «на межі» юридичної та технічної наук. Зокрема, тепер в нашому законодавстві роз'яснено що таке кібератака, кібербезпека, кіберзагроза, кіберзахист, кіберзлочин (комп'ютерний злочин), кіберзлочинність, кібероборона, кіберпростір, кіберрозвідка, кібертероризм, кібершпигунство, критична інформаційна інфраструктура [5]. Важливо зазначити також, що цей закон в загалом визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [5].

Так, відповідно до п. 9 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», під кіберзлочинністю законодавець розуміє сукупність кіберзлочинів [5]. В свою чергу, до п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [5]. Проте, в контексті піднятої нами проблематики, закцентуємо увагу на тому, що є ризик різного трактування на законодавчому рівні поняття «кіберзлочину» в національних законодавствах держав, що у свою чергу є першим викликом у боротьбі з кіберзлочинністю у сфері ЗЕД.

Щоб краще зрозуміти суть суспільних відносин, що порушуються в цьому контексті, слід надати визначення того, що таке ЗЕД в розумінні законодавця. Так, відповідно до ст. 1 Закону України «Про зовнішньоекономічну діяльність», зовнішньоекономічна діяльність – це діяльність суб'єктів господарської діяльності України та іноземних суб'єктів господарської діяльності, а також діяльність державних замовників з оборонного замовлення у випадках, визначених законами України, побудована на взаємовідносинах між ними, що має місце як на території України, так і за її межами [6]. Таким чином, під кіберзлочинністю в ЗЕД в контексті даної проблематики ми розуміємо суспільно небезпечні винні діяння фізичної осудної особи (яка досягла віку з якого настає кримінальна відповідальність), у кіберпросторі та/або з його використанням, щодо суб'єктів господарської діяльності, які є учасниками ЗЕД, і вчинюваний кіберзлочин порушує суспільні відносини у сфері здійснення суб'єктами господарювання ЗЕД. Тобто, це не просто «злам комп'ютерної техніки», «злам паролів», а комплексні ризики та наслідки, що виникають за результатами діянь зловмисників під час здійснення міжнародних електронних розрахунків, побудові логістики, проведенні тендерів, реалізації контрактів суб'єктами господарювання у сфері ЗЕД.

Зазначимо, що у 2005 році Україною було ратифіковано Конвенцію про кіберзлочинність, проте із певними застереженнями та заявами [7]. Дана конвенція слугує основою для формування законодавства у сфері боротьби з кіберзлочинністю для держав, що зробили її частиною свого законодавства. У тому числі, згадана конвенція є базою формування спільної кримінальної політики щодо захисту суспільства від кіберзлочинності [7]. Між іншим, положення даної конвенції дозволяють створювати відповідні ініціативи для налагодження міжнародного співробітництва у сфері боротьби з протиправними діями у кіберпросторі. В цьому контексті варто закцентувати увагу на необхідності спільній протидії кіберзлочинності на рівні урядів держав, оскільки кіберзлочини

не обмежені державними кордонами. Завдяки інтернет простору дії особи в будь-якій точці світу можуть мати вплив на безпеку користувачів. Адже, сервер, суб'єкт вчинення кримінального правопорушення, потерпілий перебувають під юрисдикціями різних держав.

В такому разі постає питання ефективності та оперативності розслідування, можливості швидкого встановлення винної особи та притягнення її до кримінальної відповідальності. Ми впевнені, що кожна держава світу зобов'язана не допускати використовувати свою територію для вчинення кіберзлочинів. При такому підході до вирішення даної проблематики сфера ЗЕД буде більш захищеною в розглядуваному нами контексті.

Окреслимо, такі основні тенденції у сфері кіберзлочинності що порушують суспільні відносини у сфері ЗЕД.

По-перше, варто згадати це про так званий «фішинг» та «соціальну інженерію». Зловмисні діяння у згаданому контексті проявляються у намаганні правопорушників отримати конфіденційну інформацію, персональні дані співробітників чи партнерів компанії-жертви шляхом здійснення надсилання електронного листа на офіційну електронну пошту потерпілої компанії. Згаданий нами лист надсилається разом із зашифрованим шкідливим програмним забезпеченням. Не підозрюючи цього, співробітник компанії відкриває такий лист і активує це програмне забезпечення. Як наслідок, стається витік конфіденційної інформації та персональних даних [8]. Є часті випадки того, як бізнес отримує підроблені рахунки-фактури, оплачує по ним послуги ніби то свого «контрагента», проте насправді кошти потрапляють на рахунки кіберзлочинців.

По-друге, про що варто згадати, це про злам корпоративних систем і баз даних. Переважна більшість компаній має корпоративний Wi-Fi. Варто акцентувати увагу на тому, що кожен співробітник компанії під час виконання своїх обов'язків користується цим Wi-Fi. Завдяки ньому здійснюється пошук інформації в мережі інтернет, відбувається пересилання інформації, робочих файлів, конфіденційної інформації тощо. Кіберзлочинці розуміють вразливість функціонування корпоративного Wi-Fi. Як наслідок, успішно зламують його та заволодівають необхідними даними компанії та її клієнтів [9].

По-третє, це розповсюдження шкідливих програм на комп'ютерних пристроях суб'єкта господарювання. Існує багато способів того, як це можливо дистанційно зробити, проте результат завжди один – кіберзлочинці заволодівають інформацією про бізнес рахунки компанії, і здійснюють необхідні в своїх цілях транзакції [10]. Прикладом може бути афера 2003 року, коли тисячі користувачів eBay спонукали викласти конфіденційну інформацію шляхом залякування можливим блокуванням особистих акаунтів [10].

По-четверте, це маніпуляції з міжнародними платежами. Це випадки, коли потенційний клієнт проводить платіж на основі підробленого інвойсу, який виставлений нібито від імені компанії, або псевдо-покупець не здійснює реальну оплату компанії за послуги або товар, однак надсилає суб'єкту господарювання підроблене підтвердження проведення відповідного платежу [11].

По-п'яте, про що варто згадати, – це про «промислове» шпигунство. Такі протиправні дії характеризуються метою отримання відомостей, які містять комерційну таємницю [12]. Кіберзлочинці мають широкий набір інструментів того, як можна досягти поставленої мети. Здобута інформація, документація часто виступає об'єктом продажу конкурентам або взагалі, такі «злами» виконуються на замовлення недобросовісних конкурентів [12].

Таким чином, розуміючи основні тенденції, наголосимо, що наявність цифрової залежності від певних платформ сприяє мотивації кіберзлочинцям діяти і «розвиватися» в напрямку своєї протизаконної діяльності.

Основними викликами з якими стикається бізнес у сфері ЗЕД на разі є відсутність єдиного підходу у різних держав світу до законодавчого визначення того, що є кіберзлочинами (наголосимо на тому, що Конвенція про кіберзлочинність не містить визначення того, що є кіберзлочином) та яким чином їх слід оперативно розслідувати, зважаючи на специфіку способу і місця вчинення злочинних діянь. Додатково, недостатній рівень кіберграмотності, цифрова залежність від іноземних платформ та сервісів, зростання кількості атак під час воєн і економічних криз сприяють розповсюдженню протиправних діянь в мережі інтернет. Це породжує такі ризики для учасників ЗЕД як фінансові та репутаційні втрати, витік комерційної та персональної інформації.

Висновки

1. Цифровізація бізнесових процесів у міжнародній торгівлі привносить нові ризики для суб'єктів господарювання в Україна та світі. На разі шахрайства стають все більш витонченими, неординарними, непередбачуваними. Роками в нашій державі панувала позиція, що потерпілий

бізнес сам винен, що зіштовхнувся зі шахрайством і спонукали потерпілих вирішувати свої проблеми у цивільно-правовій чи господарсько-правовій площині. Проте, у нинішніх реаліях стрімкої цифровізації відносин очевидно – підхід до вирішення цієї проблеми слід змінювати на державному рівні.

2. Держава має створювати умови, де в інтернет просторі бізнес буде почуватися захищеним та знатиме, що є компетентні органи, які оперативно реагуватимуть на кіберзлочини на території України та оперативно діятимуть в рамках своїх компетентностей та повноважень на міжнародній арені.

3. Не тільки український бізнес, а й іноземний мають почувати себе захищеними під юрисдикцією будь-якої держави світу.

Список літератури:

1. Вплив кіберзагроз на сучасне суспільство. Дані та висновки за 2022-2024 роки. *Institute for Cybersecurity and Analitics*. 24.01.2025. URL: https://icsa.team/701-701/ (дата звернення: 21.10.2025).

2. Кібератаки на український бізнес тривають: як захиститися. *Економічна правда*. 03.05.2024. URL: https://epravda.com.ua/projects/zakhyst-krainy/2024/05/03/713224/ (дата звернення: 21.10.2025).

3. Business Email Compromise: The $50 Billion Scam. *Federal bureau of investigation*. 09.06.2023. URL: https://www.ic3.gov/PSA/2023/psa230609?utm_source=chatgpt.com (дата звернення: 21.10.2025).

4. Денисюк М. Фейковий monobank у Telegram. *Forbes*. 21.10.2025. URL: https://forbes.ua/money/feykoviy-monobank-u-telegram-shakhrai-vimanili-62-mln-grn-u-blogerki-ksyushi-maneken-khto-vinen-ta-yak-mozhna-uniknuti-tsogo-20102025-33478 (дата звернення: 21.10.2025).

5. Про основні засади забезпечення кібербезпеки України : Закон України, *Верховна Рада України* від 05.10.2017, № 2163-VIII : станом на 27.03.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 21.10.2025 р.).

6. Про зовнішньоекономічну діяльність : Закон України, *Верховна Рада України* від 16.04.1991, № 959-XII : станом на 04.12.2024. URL: https://zakon.rada.gov.ua/laws/show/959-12#Text (дата звернення 21.10.2025 р.).

7. Конвенція про кіберзлочинність : *Верховна Рада України* від 07.09.2005, № 994_789. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text#Text (дата звернення 21.10.2025 р.).

8. Соціальна інженерія. *КіберBRAMA*. URL: https://stopfraud.gov.ua/cybersecurity-in-work/sotsialnyj-inzhyniryng-i317 (дата звернення: 21.10.2025).

9. Секрети кібербезпеки: ризики, пов'язані із зламом корпоративної мережі Wi-Fi. *European Business Association*. 26.07.2021. URL: https://eba.com.ua/sekrety-kiberbezpeky-ryzyky-pov-yazani-iz-zlamom-korporatyvnoyi-merezhi-wi-fi/ (дата звернення: 21.10.2025).

10. Шляхи зараження ПК шкідливими програмами. *ZillyaАнтивірус*. 21.07.2015. URL: https://zillya.ua/shlyakhi-zarazhennya-pk-shkidlivimi-programami (дата звернення: 21.10.2025).

11. Блінов Є. ІТ-шахрайство при експортно-імпортних операціях – чого варто побоюватися і як уникнути втрат?. *AgroPortal*. 16.08.2016. URL: https://agroportal.ua/blogs/itmoshennichestvo-pri-eksportnoimportnykh-operatsiyakh-chego-stoit-opasatsya-i-kak-izbezhat-poter (дата звернення: 21.10.2025).

12. Промислове шпигунство: профілактика, оперативне правове реагування. *Ligazakon*. 22.09.2016. URL: https://ips.ligazakon.net/document/EA009550 (дата звернення: 21.10.2025).

Davydiuk V. M. CYBERCRIME IN THE SPHERE OF FOREIGN ECONOMIC RELATIONS: CHALLENGES AND RISKS

The article provides a comprehensive analysis of cybercrime in the field of foreign economic activity (FEA) under the conditions of global digitalization. It is emphasized that the growing dependence of international trade on information and communication technologies is accompanied by an increase in cyber risks that pose additional threats to the economic security of the state and business entities.

The main forms of cybercrime typical for FEA participants are identified, including phishing, social engineering, unauthorized access to corporate databases, the spread of malicious software, and business email compromise (BEC) schemes. The consequences of such offenses are defined as significant financial losses, reputational damage, violations of contractual obligations, and the emergence of international commercial disputes.

Statistical data demonstrate the annual increase in the number and complexity of cyberattacks. Special attention is paid to real cases of fraud recorded in Ukraine, which confirm the urgency of the issue and the need to strengthen business cybersecurity.

It is established that the current legal framework and state mechanisms for responding to cybercrime in FEA do not fully meet modern technological challenges. The expediency of harmonizing Ukrainian legislation

with international standards, particularly the provisions of the Convention on Cybercrime, is substantiated.

The study highlights the necessity of developing effective cooperation between government bodies, law enforcement agencies, the private sector, and IT specialists to ensure comprehensive counteraction to cybercrime. It is concluded that improving the legal awareness of FEA participants, implementing modern digital protection tools, and enhancing international cooperation are key conditions for minimizing risks in cyberspace.

Key words: *cybersecurity, cybercrime, foreign economic activity, phishing, social engineering, trade secret, industrial espionage.*

Дата надходження статті: 28.10.2025
Дата прийняття статті: 20.11.2025
Опубліковано: 29.12.2025