https://www.sworldjournal.com/index.php/swj/article/view/swj22-03-014
DOI: 10.30888/2663-5712.2023-22-03-014

УДК 681.518

FUNCTIONAL-PROCESS MODELING OF REGULATORY SYSTEMS IN E-COMMERCE

ФУНКЦІОНАЛЬНО-ПРОЦЕСНЕ МОДЕЛЮВАННЯ РЕГУЛЮВАЛЬНИХ СИСТЕМ В Е-КОМЕРЦІЇ

Rusyn-Hrynyk R.R. / Русин-Гриник Р.Р.
PhD / доктор філософії, доцент
ORCID ID: 0000-0003-2895-6437
Zalutskyi Yu.V. / Залуцький Ю.В.
postgraduate / аспірант
Fedina Ya.V. / Федина Я.В.
postgraduate / аспірант
Lviv Polytechnic National University, Lviv, Bandery, 17, 79000
Національний університет «Львівська політехніка», Львів, Бандери, 17, 79000

***Анотація**. Доведено, що регулювальна система в е-комерції є складною та багатогранною структурою з різними функціями та властивостями. Аргументовано, що серед головних функцій регулювальної системи є забезпечення відповідності законодавству, керування бізнес-процесами, забезпечення кібербезпеки та управління даними та аналітикою. Обгрунтовано, що властивості цієї системи включають в себе складність, динамічність та підвищені вимоги до безпеки і конфіденційності даних. Висвітлено, що біполярна природа регулювальної системи підкреслює важливість взаємодії між суб'єктами господарювання та зовнішніми стейкхолдерами для забезпечення ефективності та стійкості е-комерції. Загальний висновок підтверджує важливість регулювальної системи в цьому секторі та її вплив на успішність та безпеку діяльності суб'єктів господарювання та задоволення потреб клієнтів.*

***Ключові слова**: е-комерція, бізнес-процеси, законодавство України, кібербезпека, регулювальна система, потреби клієнтів.*

Вступ.

Регулювальна система в е-комерції (е-комерції) – це комплекс правил, стандартів і політик, які встановлені для регулювання та контролю електронних торговельних операцій (ЕТО) та бізнес-процесів, які відбуваються в Інтернеті і у внутрішньому середовищі суб'єктів господарювання, які є учасниками ринку е-комерції. Ця система створюється органами державного управління, міжнародними організаціями, а також засновниками платформ, які надають послуги е-комерції. Ознайомлення з позиціями Ahi A.A., Sinkovics N. & Sinkovics R.R. [1], Bhaswat P [2], Mik E. [3], Ryzhik A., Slesarev V., Malcev V. & Kamishansky V. [4], Zhu, B., & Ahamat, H. [5], Akour I., Alnazzawi N., Alshurideh M., Almaiah M. A., Al Kurdi B., Alfaisal R. M. & Salloum S. [6], Al-Adwan A. S., Al-Debei M. M. & Dwivedi Y. K. [7], AlGhanboosi B., Ali S. & Tarhini A. [8], Alrammah I. & Ajlouni A.-W. [9], Argilés-Bosch J. M., Ravenda D. & Garcia-Blandón J. [10] дозволяє стверджувати, що в цілому регулювальні системи в е-комерції формуються у кількох векторах. Вектори стосуються як внутрішнього, так і зовнішнього середовищ підприємства, яке функціонує у сфері е-комерції, тобто регулювальні системи в е-комерції є комбінованими. До одних блоків цієї системи суб'єкти господарювання підлаштовуються, адаптуються, а інші формують самостійно виходячи з власних пріоритетів і можливостей.

Основний текст.

Розглянемо кожен з векторів формування регулювальної системи е-комерції.

І так, першим вектором є закони та нормативні акти, які встановлюють правила і обмеження для е-комерції. Законодавчі акти є одним із найважливіших аспектів регулювальної системи в е-комерції. Вони встановлюють правила та обмеження, яких суб'єкти господарювання повинні дотримуватися при проведенні торговельних операцій в Інтернеті. До ключових правових актів, які стосуються е-комерції в Україні належать: Закон України «Про електронний документ та електронний документообіг» № 3203-VI від 22 вересня 2011 року – регулює використання електронних документів і е-документообігу в е-комерції та інших сферах; Закон України «Про електронну комерцію» № 675-VIII від 3 вересня 2015 року – регулює питання, пов'язані з е-комерцією, включаючи е-контракти, права споживачів, захист даних і багато інших аспектів е-торгівельних операцій; Закон України «Про захист прав споживачів» 1023-XII від 12 травня 1991 року – містить положення, які стосуються захисту прав покупців в е-комерції; Закон України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року – встановлює вимоги щодо обробки та захисту персональних даних, що є важливим аспектом в е-комерції, де збираються особисті дані клієнтів; Закон України «Про електронні гроші» 1239-VI від 1 жовтня 2009 року – 1 жовтня 2009 року – регулює е-гроші та е-платіжні системи, які часто використовуються в е-комерції для здійснення платежів; Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80-V від 5 вересня 2007 року – містить вимоги до захисту інформації в інформаційно-телекомунікаційних системах, які використовуються в е-комерції; Закон України «Про застосування касових апаратів при реалізації товарів та послуг» № 265/95-ВР від 22 грудня 1995 року – стосується застосування касових апаратів в торговельних точках, включаючи он-лайн-магазини та інтернет-продажі тощо.

Одним з векторів, у якому формується регулювальна система у сфері е-комерції є стандарти безпеки. Стандарти визначають вимоги до захисту і безпеки даних споживачів і бізнес-процесів в інтернет-торгівлі. Основні аспекти стандартів безпеки в е-комерції включають наступне:

1) шифрування даних. Це ключовий елемент безпеки в е-комерції. Стандарти вимагають використання шифрування для захисту конфіденційних інформаційних відомостей, таких як особисті дані клієнтів та платіжна інформація;

2) захист від злому та кібератак. Стандарти встановлюють вимоги до захисту від злому та кібератак, включаючи вимоги до відстеження та реагування на можливі порушення безпеки;

3) управління доступом. Цей аспект визначає, як керувати доступом до систем та даних, що передбачає встановлення вимог до паролів, багаторівневих аутентифікаційних систем і керування правами доступу;

4) сертифікація та аудит безпеки. Деякі стандарти, як наприклад PCI DSS (Payment Card Industry Data Security Standard), вимагають сертифікації та регулярних аудитів безпеки, щоб перевірити відповідність бізнесу вимогам

безпеки [11]. Окрім PCI DSS, існують ще й інші стандарти та програми сертифікації та аудиту безпеки, які використовуються для забезпечення безпеки в е-комерції та інших сферах. Деякі з них включають: ISO/IEC 27001 – цей стандарт визначає системи управління інформаційною безпекою та вимоги до їх впровадження. Він орієнтований на всі види організацій і вимагає встановлення, реалізації, підтримки та постійного вдосконалення системи управління інформаційною безпекою; SOC 2 (Service Organization Control 2) – це стандарт, розроблений Американським товариством аудиторів (AICPA), що стосується безпеки, доступності, обробки даних та конфіденційності в організаціях, які надають послуги у сфері е-комерції [12]; HIPAA (Health Insurance Portability and Accountability Act) – це стандарт, який регулює безпеку та конфіденційність медичних даних в США. Він застосовується до медичних організацій та компаній, які обробляють медичні дані, включаючи ті, що стосуються е-комерції у сфері охорони здоров'я [13]; GDPR (General Data Protection Regulation) – це стандарт щодо захисту особистих даних громадян ЄС. Він встановлює вимоги до збору, обробки та збереження особистих даних та може стосуватися підприємців, що працюють сфері е-комерції, які мають клієнтів у ЄС [14]; FISMA (Federal Information Security Management Act) – це американський закон, який встановлює вимоги до інформаційної безпеки федеральних установ та організацій. Він має значення для е-комерції, яка стосується урядових контрактів [15]; CSA STAR (Cloud Security Alliance Security Trust Assurance and Risk) – це програма сертифікації безпеки хмарних послуг, яка допомагає користувачам хмарних сервісів оцінювати і забезпечувати безпеку в хмарному середовищі [16]. Ці стандарти та програми сертифікації допомагають організаціям та бізнесам дотримуватися вимог безпеки та захисту даних у своїх операціях, включаючи е-комерцію. Вибір конкретного стандарту залежить від потреб та особливостей бізнес-процесів суб’єкта господарювання;

5) захист від фішингу та шахрайства. Фішинг (англ. Phishing) – це вид кіберманіпуляції або шахрайства, коли злочинець намагається обманом отримати конфіденційну інформацію, таку як паролі, номери кредитних карт, соціальні номери, або інші особисті дані від жертви. Фішери (особи, які виконують фішинг) зазвичай представляють себе як надійне джерело, якими можуть бути банки, компанії, або навіть урядові органи, щоб переконати жертву надати їм свої особисті дані. Мета фішингу – викрасти особисті дані або гроші, і тому важливо бути обережним та пильним при отриманні надзвичайно схожих запитів на введення конфіденційної інформації. Для захисту від фішингу рекомендується перевіряти автентичність джерел та запитів, не надавати особисті дані без перевірки, використовувати надійні паролі та бути уважними при взаємодії з невідомими джерелами. Розрізняють такі види фішингу: фішинг е-поштою (злочинці надсилають е-листи, що виглядають як листи від відомих компаній або організацій, і просять жертву перейти на підроблену веб-сторінку та ввести свої дані); фішинг через соціальні мережі (злочинці створюють підроблені облікові записи або сторінки в соціальних мережах та намагаються віддалено здійснити з жертвами спілкування, щоб отримати їхні особисті дані або гроші); фішинг на веб-сайтах (фішери створюють підроблені веб-сайти, які

схожі на офіційні сторінки банків або інших організацій, та намагаються переконати жертву ввести свої дані); фішинг телефоном (фішери намагаються зателефонувати жертвам, вигідно розмовляти з ними і виманювати конфіденційну інформацію); фішинг через текстові повідомлення (смісервіси) (злочинці надсилають SMS-повідомлення, що виглядають як повідомлення від банків або інших організацій, і просять жертву перейти за посиланням або відповісти на повідомлення);

6) захист даних клієнтів. Стандарти вимагають від суб'єктів господарювання у сфері е-комерції дотримуватися правил щодо збереження та обробки особистих даних клієнтів, включаючи вимоги до знищення даних, коли вони більше не потрібні.

Дотримання стандартів безпеки є важливим для підтримання довіри споживачів і запобігання порушенням безпеки в е-комерції. Підприємці повинні дотримуватися відповідних стандартів, щоб забезпечити надійний та безпечний досвід покупців в інтернет-магазинах.

Серед векторів формування регулювальних систем в е-комерції виділено також податкову політику, яка визначає правила і обов'язки щодо оподаткування ЕТО і може включати такі аспекти:

- податок на додану вартість (ПДВ) та інші податки. Багато країн вимагають, щоб е-торговельні операції підлягали оподаткуванню ПДВ або подібними податками. ПДВ зазвичай застосовується до вартості товарів і послуг, проданих в е-магазинах. Податкова ставка і умови сплати податку можуть варіюватися в залежності від країни. Ось деякі приклади країн, де е-торговельні операції підлягають оподаткуванню ПДВ або подібними податками: У багатьох країнах ЄС існує система податку на додану вартість (VAT), яка застосовується до ЕТО. ЄС також впроваджує нові правила для оподаткування е-послуг та продажів он-лайн-товарів в межах єдиного цифрового ринку. Деякі штати у США встановлюють збір з продажу (Sales Tax) на е-торгівельні операції. У Канаді існує ГСТ (загальний податок на оборот) і ПСТ (продажний податок), які можуть бути застосовані до е-комерції, залежно від провінції. У Австралії діє податок на товари і послуги (Goods and Services Tax - GST), який застосовується до багатьох ЕТО. В Індії діє подібна система податку на товари і послуги (Goods and Services Tax - GST), яка охоплює е-комерцію. Китай також має свою систему податку на товари і послуги (Value Added Tax - VAT), яка визначає ставки для е-комерції. У Японії існує система споживчого податку (Consumption Tax), яка застосовується до товарів і послуг, включаючи е-комерцію;
- місце оподаткування. Податкове законодавство часто визначає місце оподаткування для ЕТО, особливо у випадках, коли покупці і продавці розташовані в різних країнах або регіонах. Питання місця оподаткування є важливим аспектом оподаткування ЕТО, особливо в контексті міжнародних торговельних операцій. Місце оподаткування визначає, в якій країні або регіоні буде обчислюватися і сплачуватися податок на е-торговельні операції. В основному існують два підходи до визначення місця оподаткування, яке більш зручне для: *покупця (Destination Principle)*. За цим підходом місце оподаткування визначається на основі місця розташування покупця. Це означає, що податок

обчислюється згідно з податковими ставками і правилами, що діють у країні або регіоні, де знаходиться покупець. Цей підхід зазвичай застосовується для споживчих товарів і послуг. Наприклад, якщо покупець з США (де діє збір з продажу) здійснює покупку у веб-магазині, розташованому в Європейському Союзі (де діє ПДВ), то податок буде обчислюватися відповідно до ставок і правил ЄС, оскільки місцем оподаткування є країна покупця (США) [17]; *продавця (Origin Principle)*. За цим підходом місце оподаткування визначається на основі місця розташування продавця. Це означає, що податок обчислюється згідно з податковими ставками і правилами, які діють у країні або регіоні, де знаходиться продавець. Цей підхід зазвичай використовується для бізнес-до-бізнес (B2B) транзакцій. Наприклад, якщо компанія з Європейського Союзу (де діє ПДВ) продає товари іншій компанії в США, то податок буде обчислюватися відповідно до ставок і правил ЄС, оскільки місцем оподаткування є країна продавця (ЄС). Вибір місця оподаткування може впливати на обсяги податку, який підприємство повинно сплатити, і вимагає від суб'єктів господарювання дотримуватися складних правил і вимог. Тому важливо мати чітке розуміння правил оподаткування в кожній конкретній ситуації, особливо в міжнародному контексті [18]. У законодавстві різних країн та регіонів ці підходи (Destination Principle і Origin Principle) можуть бути згадані під різними назвами, і не завжди вони фіксуються у окремих законодавчих актах з конкретними назвами. Зазвичай, це визначається загальними принципами оподаткування та правилами, які стосуються е-комерції в кожній окремій юрисдикції. Наприклад, в контексті ЄС, підходи Destination Principle і Origin Principle відображаються в системі оподаткування ПДВ для ЕТО. Згідно з правилами ЄС, для споживчих операцій застосовується Destination Principle, тобто податок обчислюється відповідно до місця розташування покупця (країни покупця). Для бізнес-до-бізнес операцій застосовується Origin Principle, де податок обчислюється відповідно до місця розташування продавця. Конкретні законодавчі акти та документи, які регулюють ці питання в ЄС, можуть змінюватися з часом, і їх назви можуть варіюватися. Наприклад, Директива ЄС 2006/112/ЕС встановлює загальні правила щодо ПДВ в ЄС, але після реформ в 2015 році було введено нові правила для оподаткування е-послуг та продажів он-лайн-товарів в рамках єдиного цифрового ринку [19];

- облік і звітність. Суб'єкти господарювання, які здійснюють е- комерцію, можуть бути зобов'язані вести облік та представляти звіти про свої торговельні операції для цілей оподаткування. Це може включати ведення обліку стосовно ПДВ, відстеження продажів і закупівель, а також звітність перед податковими органами;
- податкові звіти і платежі. Суб'єкти господарювання зазвичай повинні регулярно подавати податкові звіти та внески, щоб виплачувати податки на прибуток, ПДВ і інші податки;
- податкові пільги та звільнення від податків. Деякі країни надають пільги або звільнення від податків для підприємств у сфері е-комерції, особливо для суб'єктів малого бізнесу;

Ще одним вектором формування регулювальної системи в е-комерції є захист споживачів. Захист споживачів спрямований на відстоювання інтересів споживачів, які здійснюють покупки та торговельні операції в он-лайн-середовищі. У даному контексті ключовими питаннями є такі: *право на інформацію* (у сфері е-комерції, продавці повинні надавати споживачам вичерпну та доступну інформацію про товари і послуги, що пропонуються. Це включає в себе ціни, властивості товарів, умови доставки, правила повернення та іншу інформацію, яка допомагає споживачам приймати обдумані рішення. Споживачі в Україні мають право на одержання вичерпної та доступної інформації про товари і послуги, які пропонуються в е-комерції. Це визначено в «Законі України про захист прав споживачів» та в інших законодавчих актах); *право на відмову від покупки і повернення товарів* (споживачі зазвичай мають право відмовитися від покупки і повернути товари протягом певного строку після отримання. Це дозволяє споживачам випробовувати товари та переконатися, що вони відповідають їхнім очікуванням. Правила повернення можуть варіюватися в залежності від країни і типу товару. Законодавство України передбачає право споживачів на відмову від покупки та повернення товарів, якщо це не суперечить встановленим умовам. Це право регулюється «Законом України про захист прав споживачів»); *захист від обманливої реклами* (законодавство може включати правила щодо реклами та маркетингу в е-комерції, щоб запобігти обманливим практикам та забезпечити чесну інформацію для споживачів. Закон України «Про рекламу» містить норми, які стосуються запобігання обманливій рекламі та забезпечення чесної інформації для споживачів); *захист особистих даних* (закони про захист особистих даних можуть забезпечувати споживачам контроль над їхніми особистими даними, які збираються та обробляються в е-комерції. Охорона особистих даних в е-комерції регулюється Законом України «Про захист особистих даних», який визначає правила обробки особистих даних та забезпечення їх безпеки); *безпека платежів і транзакцій* (забезпечення безпеки платежів та транзакцій включає в себе використання шифрування та стандартів безпеки, щоб уникнути зловживання платіжних даних. Забезпечення безпеки платежів та транзакцій в Україні також регулюється законодавством та нормами щодо електронних платежів і фінансових послуг). Правила і норми захисту споживачів можуть відрізнятися в кожній країні, але їхня мета полягає в тому, щоб гарантувати права та безпеку споживачів під час ЕТО. Суб'єкти господарювання, що займаються е-комерцією, повинні дотримуватися цих правил і норм, щоб забезпечити довіру споживачів та уникнути юридичних проблем.

Вектором формування регулювальної системи в е-комерції є також ліцензування та реєстрація, що супроводжуються вимогами та процедурами, які підприємства в сфері е-комерції повинні виконувати для провадження своєї діяльності. Так, деякі види діяльності в е-комерції можуть вимагати ліцензування. Це включає ліцензії на провадження операцій з платежами, обробку фінансових транзакцій, продаж алкогольних або тютюнових товарів тощо. Ліцензії встановлюються відповідно до законодавства кожної конкретної країни або регіону.

В Україні реєстрація підприємств, які займаються е-комерцією, є важливою частиною їх легального функціонування. Основними аспектами реєстрації підприємств в України є:

1. *Реєстрація бізнесу.* Підприємства, що здійснюють е-комерцію, повинні бути зареєстровані як юридичні особи або підприємці відповідно до законодавства України. Реєстрація бізнесу проводиться в органах державної реєстрації, зазвичай у формі державної реєстрації юридичних осіб або фізичних осіб-підприємців. В Україні процедура реєстрації бізнесу проводиться через органи державної реєстрації. Основні органи, які відповідають за реєстрацію бізнесу в Україні, включають наступні: *Державна реєстраційна служба України* (головний орган, відповідальний за проведення державної реєстрації юридичних осіб та фізичних осіб - підприємців в Україні. Ця Служба забезпечує видачу свідоцтв про державну реєстрацію юридичних осіб та індивідуальних підприємців); *Державна служба статистики України* (відповідає за надання суб'єктам господарювання ідентифікаційних номерів, які використовуються для статистичного обліку і звітності перед державою); *Податкова служба України* (видає податковий ідентифікаційний номер (ІПН) платника податків, який необхідний для реєстрації бізнесу та сплати податків); *Місцеві органи виконавчої влади та місцевого самоврядування* (деякі аспекти реєстрації бізнесу, зокрема отримання дозволів та ліцензій, можуть залежати від конкретного регіону або міста, де знаходиться бізнес). Для проведення реєстрації бізнесу в Україні, підприємці зазвичай звертаються до відповідних відділів Державної реєстраційної служби та інших органів, які надають необхідну інформацію та послуги для реєстрації бізнесу та отримання необхідних документів.

2. *Отримання ідентифікаційних номерів*. Підприємства повинні отримати ідентифікаційні номери для оподаткування та роботи з державними органами. Це включає в себе ідентифікаційний номер платника податків (ІПН), а також інші номери, які необхідні для співпраці з органами регулювання та фіскальними органами.

3. *Податковий реєстр*. Підприємства зареєструються в податковому реєстрі, декларують та сплачують податки відповідно до податкового законодавства України.

4. *Реєстрація фінансових операцій*. У деяких випадках, зокрема, якщо е-магазин приймає платежі від споживачів або здійснює фінансові операції, може бути потрібно реєструватися в Національній комісії, що здійснює регулювання ринків фінансових послуг.

Висновки. Правові акти визначають різні аспекти е-комерції в Україні, включаючи права та обов'язки суб'єктів господарювання, захист даних, платіжні системи, авторські права, застосування е-підпису і багато інших аспектів цього виду діяльності. Загалом, законодавчі акти в е-комерції визначають правовий фреймворк, який допомагає створити чесні та довірені відносини між суб'єктами підприємництва в е-комерції та споживачами, забезпечити права та захист інтересів усіх сторін і досягти стабільності та надійності здійснення ЕТО.

Важливо, щоб суб'єкти господарювання, які займаються е-комерцією, дотримувалися податкових вимог та правил у своїй країні та в інших країнах, де

вони продають товари або послуги. Реєстрація підприємства та дотримання податкових та регуляторних вимог допомагає забезпечити легальну та безпечну діяльність у сфері е-комерції в Україні.

Література.

1. Ahi, A.A., Sinkovics, N. & Sinkovics, R.R. (2023). E-commerce Policy and the Global Economy: A Path to More Inclusive Development? Manag Int Rev 63, p.p. 27–56. https://doi.org/10.1007/s11575-022-00490-1 .

2. Prakash, Bhaswat, (2023). A Legal and Compliance Framework on Latest E – Commerce Rules and Regulation for the Protection and Welfare of both the Consumer and Seller with respect to Platforms (June 9, 2023). Available at SSRN: https://ssrn.com/abstract=4474251 or http://dx.doi.org/10.2139/ssrn.4474251 .

3. Mik, Eliza, (2017). Legal and Regulatory Challenges to Facilitating E-Commerce in the ASEAN (December 1, 2017). Available at SSRN: https://ssrn.com/abstract=3100578 or http://dx.doi.org/10.2139/ssrn.3100578 .

4. RYZHIK, A., SLESAREV, V., MALCEV, V., & KAMISHANSKY, V. (2020). Website as an e-Commerce Tool: Regulatory Technology. Journal Of Advanced Research In Law And Economics, 11(3), 1032 – 1038. doi:10.14505/jarle.v11.3(49).37 .

5. Zhu, B., & Ahamat, H. (2023). The Role of E-commerce Adoption in Enhancing Regulatory Compliance in Information Systems of Foreign Investment Management in Malaysia - A Moderating Effect of Innovation Management. Journal of Information Systems Engineering and Management, 8(3), 21797. https://doi.org/10.55267/iadt.07.13611 .

6. Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S. (2022). A Conceptual Model for Investigating the Effect of Privacy Concerns on E-Commerce Adoption: A Study on United Arab Emirates Consumers. Electronics, 11(22), 3648. https://doi.org/10.3390/ELECTRONICS11223648 .

7. Al-Adwan, A. S., Al-Debei, M. M., & Dwivedi, Y. K. (2022). E-commerce in high uncertainty avoidance cultures: The driving forces of repurchase and word-of-mouth intentions. Technology in Society, 71, 102083. https://doi.org/10.1016/j.techsoc.2022.102083.

8. AlGhanboosi, B., Ali, S., & Tarhini, A. (2023). Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. Computers in Human Behavior, 144, 107702. https://doi.org/10.1016/j.chb.2023.107702 .

9. Alrammah, I., & Ajlouni, A.-W. (2021). A framework and a Zhu B. et al. / J INFORM SYSTEMS ENG, 8(3), 21797 14 / 17 survey analysis on nuclear security culture at various radiological facilities. Annals of Nuclear Energy, 158, 108294. https://doi.org/10.1016/j.anucene.2021.108294 .

10. Argilés-Bosch, J. M., Ravenda, D., & Garcia-Blandón, J. (2021). E-commerce and labour tax avoidance. Critical Perspectives on Accounting, 81, 102202. https://doi.org/10.1016/j.cpa.2020.102202 .

11. Williams, B., & Adamson, J. (2022). PCI Compliance: Understand and

Implement Effective PCI Data Security Standard Compliance (5th ed.). CRC Press. https://doi.org/10.1201/9781003100300 /

12. Soc2 - service organization control 2 by the american institute of cpas (aicpa) https://www.isomanager.com/soc2-service-organization-control-2-by-the-american-institute-of-cpas-aicpa.html .

13. Krzyzanowski, B., & Manson, S. M. (2022). Twenty Years of the Health Insurance Portability and Accountability Act Safe Harbor Provision: Unsolved Challenges and Ways Forward. JMIR medical informatics, 10(8), e37756. https://doi.org/10.2196/37756 .

14. Dove, E. S. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law, Medicine & Ethics, 46(4), 1013-1030. https://doi.org/10.1177/1073110518822003 .

15. Hulitt, E., Vaughn, R.B. Information system security compliance to FISMA standard: a quantitative measure. Telecommun Syst 45, 139–152 (2010). https://doi.org/10.1007/s11235-009-9248-8 .

16. Minimize risk and inspire trust with csa star certification https://www.tuvsud.com/en-us/services/auditing-and-system-certification/csa-star .

17. European Commission, Directorate-General for Taxation and Customs Union, Jaras, T., Whittle, E., Patel, K. et al., Implementing the 'destination principle' to intra-EU B2B supplies of goods – Feasibility and economic evaluation study – Final report, Publications Office, 2015, https://data.europa.eu/doi/10.2778/216975 .

18. Cavaliere, Paolo, (2021). Who's Sovereign? The AVMSD's Country of Origin Principle and Video-sharing Platforms (December 15, 2021). Journal of Digital Media & Policy, vol. 12 Issue 3 407-423, Edinburgh School of Law Research Paper No. 23, Available at SSRN: http://dx.doi.org/10.2139/ssrn.3986101 .

19. Michael Keen, Sajal Lahiri, (1998). The comparison between destination and origin principles under imperfect competition, Journal of International Economics, Vol. 45, Issue 2, Pages 323-350, ISSN 0022-1996, https://doi.org/10.1016/S0022-1996(98)00005-1 .

Abstract. *It has been proven that the regulatory system in e-commerce is a complex and multifaceted structure with various functions and properties. It is argued that among the main functions of the regulatory system are ensuring compliance with legislation, managing business processes, ensuring cyber security and managing data and analytics. It is justified that the properties of this system include complexity, dynamism and increased requirements for data security and confidentiality. It is highlighted that the bipolar nature of the regulatory system emphasizes the importance of interaction between business entities and external stakeholders to ensure the efficiency and sustainability of e-commerce. The general conclusion confirms the importance of the regulatory system in this sector and its impact on the success and safety of business entities and meeting the needs of customers.*

Keywords: *e-commerce, business processes, legislation of Ukraine, cyber security, regulatory system, customer needs.*

Науковий керівник: PhD, доцент Русин-Гриник Р.Р.
Стаття подана до друку 09.11.2023р.