Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет інформаційно-аналітичних технологій та менеджменту
(повна назва)
Кафедра економічної кібернетики та управління економічною безпекою
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Управління безпекою діяльності e-commerce підприємств
(тема)

Виконав:
студент 2 курсу, групи УФЕБм-21-1
Петренко М.А.
(прізвище, ініціали)

Спеціальність 073 Менеджмент
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Управління фінансово-економічною безпекою
(повна назва освітньої програми)
Керівник доц. Кирій В.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Полозова Т.В.
(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет__інформаційно-аналітичних технологій та менеджменту_____

Кафедра__економічної кібернетики та управління економічною безпекою___
(повна назва)

Рівень вищої освіти _другий (магістерський)_____

Спеціальність _073 Менеджмент_____
(код і повна назва)

Тип програми_освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)

Освітня програма Управління фінансово-економічною безпекою_____
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри
_____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові__Петренку Максиму Андрійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи __Управління безпекою діяльності e-commerce підприємств
_____
_____
затверджена наказом по університету від 07 листопада 2022 р. № 1452 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 19 грудня 2022 р.
3. Вихідні дані до роботи Фінансова звітність підприємства, періодичні видання, наукова література, інформаційні ресурси мережі Інтернет.
_____
_____
_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі Вступ. 1. Теоретично- методологічні аспекти управління безпекою e-commerce підприємств. 2. Аналіз та тенденції розвитку e-commerce. 3. Удосконалення управління безпекою e-commerce підприємств. Висновки. Перелік джерел посилання. Додаток.
_____
_____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

1. Об'єкт, предмет, мета і завдання дослідження, наукові результати. 2. Узагальнення понять електронна комерція 3. Характеристика періодів розвитку електронної комерції 4-5. Основні тенденції електронної комерції 6-7. Основні тенденції електронної комерції в Україні 8-11. Механізм ідентифікації та управління ризиками e-commerce».

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	07.11. 2022-12.11. 2022	виконано
2	Виконання другого розділу роботи	13.11. 2022-20.11. 2022	виконано
3	Виконання третього розділу роботи	21.11. 2022-02.12. 2022	виконано
4	Оформлення роботи	03.12. 2022-09.12. 2022	виконано
5	Перевірка роботи на плагіат	10.12. 2022-13.12. 2022	виконано
6	Підготовка доповіді та ілюстративного матеріалу	14.12. 2022-16.12. 2022	виконано
7	Рецензування роботи	17.12.2022-18.12. 2022	виконано
8	Подання роботи до екзаменаційної комісії	19.12.2022	виконано

Дата видачі завдання __07 листопада___2022 р.

Студент _____
(підпис)

Керівник роботи _____ _____доц. Кирій В.В._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Кваліфікаційна робота: 90 с., 10 табл., 25 рис., 73 джерела, 1 додаток.

E-COMMERCE, РИЗИКИ, УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ СИСТЕМ, МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ.

Об’єктом дослідження є управління системою фінансово-економічної безпеки e-commerce підприємства.

Метою роботи є теоретичне обґрунтування та розробка практичних рекомендацій щодо заходів для забезпечення безпеки діяльності e-commerce підприємства на основі ідентифікації та управління ризиками.

Розглянуто теоретичні основи управління та організація безпеки діяльності e-commerce.

Проаналізовано динаміку та результати функціонування e-commerce підприємств у світі та в Україні. Визначені тенденції розвитку галузі. Розглянуто особливості забезпечення безпеки діяльності підприємств e-commerce. Визначені напрями удосконалення управління ризиками під час функціонування e-commerce операцій.

ABSTRACT

Master’s thesis: 90 p., 10 tables, 25 fig., 73 sources, 1 exhibit.

E-COMMERCE, RISKS, INFORMATION SYSTEM SECURITY MANAGEMENT, RISK MANAGEMENT METHODS.

The object of the study is the management of the financial and economic security system of the e-commerce enterprise.

The purpose of the work is theoretical substantiation and development of practical recommendations for measures to ensure the security of e-commerce activities of the enterprise based on identification and risk management.

The theoretical foundations of management and organization of security of e-commerce activities are reviewed.

The dynamics and results of the functioning of e-commerce enterprises in the world and in Ukraine are analyzed. The development trends of the industry have been determined. The peculiarities of ensuring the security of e-commerce enterprises are considered. Areas of improvement of risk management during the functioning of e-commerce operations have been determined.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ІВ – інтелектуальна власність;

УІВ – управління інтелектуальною власністю;

CI – competitive intelligence.

ВСТУП

Кілька останніх десятиліть відбуваються активні процеси глобалізації суспільства. Глобалізація має місце у різних сферах, але найбільш яскраво вона спостерігається у інформаційно-комунікаційній сфері. Створено глобальні комунікації і глобальні соціальні мережі. Банківські розрахунки і торгівля здійснюються через комп'ютери і смартфони. Великий обсяг торговельних і фінансових операцій відбувається саме через мережу Інтернет. Як наслідок, електронна комерція є сферою, у якій постійно створюються нові робочі місця, що говорить про її значну соціалізацію. У період пандемії COVID-19 розвиток електронної комерції продовжує зростати, що викликано обмеженнями щодо відвідування громадських місць і перетину кордону.

Останніми роками в Україні сформувалось кілька IT центрів національного масштабу у Києві, Харкові, Одесі тощо. Завдяки розвитку IT сфери все більша кількість підприємців стають суб'єктами електронної комерції, при цьому зростає обсяг експорту високотехнологічних послуг, величина сплачених у державний бюджет податків і, в цілому, зростає середній рівень кваліфікації зайнятого населення. З огляду на це, актуальним є своєчасно виявляти світові тренди розвитку електронної комерції, особливо в контексті можливостей для України та стрибкоподібного зростання обсягів електронної торгівлі протягом останніх двох років.

Дослідженням питань розвитку електронної комерції в Україні займалися ряд вчених-економістів. В своїх працях вони досліджували різні сторони електронної комерції, економічні принципи, маркетинг, систему продажів та просування, ефективність реклами, дослідження управління персоналом на підприємствах електронної комерції. Досить значна кількість робіт була присвячена технічним та технологічним особливостям процесу

електронної торгівлі. Проте, не дивлячись на це, є питання, що потребують подальшого розвитку, а саме питання, по’вязані з економічною безпекою діяльності підприємств електронної комерції, виявлення та оцінювання ризиків такої діяльності.

Об’єктом дослідження є процес управління системою фінансово-економічної безпеки e-commerce підприємства.

Предметом дослідження є сукупність теоретичних і науково-методичних аспектів оцінки ризиків діяльності підприємств e-commerce.

Метою роботи є теоретичне обґрунтування та розробка практичних рекомендацій щодо заходів для забезпечення безпеки діяльності e-commerce підприємства на основі ідентифікації та управління ризиками.

Задачі роботи:

– розкрити особливості електронної комерції;

– визначити складові стану безпеки електронної комерції;

– проаналізувати методи управління ризиками для інформаційних систем в електронній комерції;

– проаналізувати тенденції розвитку e-commerce;

– запропонувати механізм ідентифікації та управління ризиками безпеки функціонування e-commerce;

– розробити заходи щодо оцінки та управління ризиками.

Методичною основою для проведення дослідження є вітчизняні та іноземні джерела: монографії, збірники та навчальні посібники з інтелектуальної власності, статті в періодичних виданнях і тези доповідей на наукових конференціях, звіти дослідницьких компаній, аналітичні матеріали, офіційна статистична звітність, галузеві веб-ресурси і профільні інтернет-видання, також законодавство України.

Для досягнення поставлених у роботі цілей використовуються такі методи: системного аналізу; аналітичного порівняння; синтезу та інші загальноприйняті методи економічного дослідження.

Апробація результатів дослідження. Основні теоретичні положення та практичні результати проведених досліджень, висновки та рекомендації, які викладені в роботі, доповідались на ІІІ Міжнародній науково-практичній конференції «Сучасні стратегії економічного розвитку: наука, інновації та бізнес-освіта», Харків, ХНУРЕ, 2022. Окремі положення роботи опубліковано у тезах. На основі проведених досліджень було представлено статтю у колективній монографії «Сучасні тенденції сталого розвитку: теорія, методологія, практика».

1 ТЕОРЕТИЧНО- МЕТОДОЛОГІЧНІ АСПЕКТИ УПРАВЛІННЯ БЕЗПЕКОЮ E-COMMERCE ПІДПРИЄМСТВ

1.1 Характеристика поглядів на електронну комерцію

Електронна комерція (e-commerce) — це купівля та продаж товарів і послуг або передача коштів або даних через електронну мережу, переважно через Інтернет. Розвиток електронної комерції значною мірою залежить від технічної інфраструктури та технологій електронних платежів, а також від рівня безпеки транзакцій. Крім того, в сучасних умовах розвиток електронної комерції значною мірою визначається інфраструктурою систем кодування та ідентифікації інформації про товари, підприємства, логістичні операції. Як динамічна бізнес-модель, електронна комерція розвивається швидкими темпами та охоплює все більше нових операцій і процесів:

– встановлення контакту (не фізичного) між «покупцем» і «продавцем»;

– обмін комерційною інформацією;

– повний цикл інформаційної підтримки покупця;

– пошук, демонстрація, вибір, консультація, конкурентоспроможність продукції;

– продаж товарів, у тому числі електронних виробів, рендеринг послуги;

– взаєморозрахунки (у тому числі за допомогою електронних грошових переказів, кредитних карток, електронних грошей);

– управління процесом доставки товару безпосередньо покупцю або за вказаною ним адресою;

– післяпродажне обслуговування [1].

Вчені мають різні погляди на сутність поняття «електронна комерція». Узагальнення понять представлено в табл.1.1.

Таблиця 1.1 – Узагальнення понять «електронна комерція»

Автори	Авторські позиції
Д. Козьє [2]	«…електронна комерція включає не лише купівлю-продаж товарів та послуг через Інтернет … у це поняття також входить підтримка отримання прибутку, створення попиту на товари та послуги, впровадження 42після продажного обслуговування клієнтів полегшення взаємодії між діловими партнерами….»
А. Мартовий [3]	«… електронна комерція – це технологія, яка забезпечує повний замкнутий цикл операцій, який включає замовлення товару, проведення платежів, участь в управлінні доставкою товару переважно орієнтовану на отримання прибутку в результаті угод і транзакцій в Інтернеті….»
Г. Хубаєв [4]	«…електронна комерція є формою постачання продукції, при якій вибір і замовлення товарів здійснюється через комп'ютерні мережі, а розрахунки між покупцем і постачальником здійснюється з використанням електронних документів і засобів платежу…»
N. Boreyko, Yu. Kovalenko, T. Krasnova [5]	«…розвиток електронної комерції … пов'язаний з поширенням мережі Інтернет, адже кількість інтернет-користувачів прямо пропорційно впливає на кількість потенційних покупців у інтернет-магазинах … проте низький рівень купівельної спроможності громадян гальмує розвиток електронної комерції…»
Y. Nanehkaran [6]	«…електронна комерція … докорінно змінює течію людського життя … є одним з головних критеріїв революції … що … змінила традиційний бізнес. Ці зміни є основою для будь-якого рішення в економіці…»
Summer, Gr. Dunkan [7]	«…електронна комерція – це форма бізнесу, яка передбачає взаємодію між суб'єктами електронним шляхом з використанням Інтернет-технологій…»

За останні два десятиліття широке використання платформ електронної комерції, таких як Amazon і eBay, сприяло значному зростанню роздрібної онлайн-торгівлі. За даними Бюро перепису населення США, у 2011 році електронна комерція становила 5% від загального обсягу роздрібних продажів. До 2020 року, з початком пандемії COVID-19, він зріс до понад 16% роздрібних продажів.

Платформи, на яких здійснюються транзакції електронної комерції, включають онлайн-ринки, на яких реєструються продавці, наприклад Amazon; програмне забезпечення як послуга (SaaS), інструменти, які дозволяють клієнтам «орендувати» інфраструктури онлайн-магазинів; або інструменти з відкритим кодом , якими компанії керують за допомогою своїх власних розробників.

Як і у традиційному ринку бувають різні види ринків, так і в системі електронної комерції є різні ринки.

Електронна комерція « бізнес-бізнес» (B2B) означає електронний обмін продуктами, послугами чи інформацією між підприємствами, а не між підприємствами та споживачами. Приклади включають онлайн-довідники та веб-сайти обміну товарами та товарами, які дозволяють підприємствам шукати продукти, послуги та інформацію та ініціювати операції через інтерфейси електронних закупівель. У звіті Forrester, опублікованому в 2018 році, передбачено, що до 2023 року B2B електронна комерція досягне 1,8 трильйона доларів і становитиме 17% продажів B2B в США.

Бізнес-споживач (B2C) – це роздрібна частина електронної комерції в Інтернеті. Це коли підприємства продають продукти, послуги чи інформацію безпосередньо споживачам. Цей термін був популярний наприкінці 1990-х років, коли онлайн-магазини та продавці товарів були в новинку. Сьогодні в Інтернеті є незліченна кількість віртуальних магазинів і торгових центрів, де продаються всі види споживчих товарів. Amazon є найбільш відомим прикладом таких сайтів. Він домінує на ринку B2C.

Від споживача до споживача (C2C) — це тип електронної комерції, у якому споживачі обмінюються продуктами, послугами та інформацією один з одним в Інтернеті. Ці транзакції зазвичай здійснюються через третю сторону, яка надає онлайн-платформу, на якій здійснюються транзакції.

Онлайн-аукціони та рекламні оголошення є двома прикладами платформ C2C. EBay і Craigslist є двома добре відомими прикладами цих платформ. Оскільки eBay – це бізнес, цю форму електронної комерції також можна назвати C2B2C – від споживача до підприємства – споживачу. Такі платформи, як Facebook Marketplace і Depop – платформа для перепродажу моди – також уможливлюють транзакції C2C.

Споживач-бізнес (C2B) – це тип електронної комерції, у якому споживачі роблять свої продукти та послуги доступними в Інтернеті для

компаній, які можуть робити ставки та купувати. Це протилежність традиційній комерційній моделі B2C. Популярним прикладом платформи C2B є ринок, який продає безоплатні фотографії, зображення, медіа та елементи дизайну, такі як iStock. Іншим прикладом може бути дошка вакансій.

Бізнес-адміністрація (B2A) відноситься до транзакцій, які здійснюються в Інтернеті між компаніями та органами державного управління чи уряду. Багато гілок влади залежать від різних видів електронних послуг або продуктів. Ці продукти та послуги часто стосуються юридичних документів, реєстрів, соціального страхування, податкових даних і зайнятості. Підприємства можуть надавати їх в електронному вигляді. Послуги B2A значно зросли за останні роки завдяки інвестиціям у можливості електронного урядування.

Споживач до адміністрації (C2A) відноситься до транзакцій, які здійснюються в Інтернеті між споживачами та органами державного управління чи уряду. Уряд рідко купує продукти чи послуги у фізичних осіб, але люди часто використовують електронні засоби в таких сферах:

Мобільна електронна комерція (m-commerce) стосується онлайн-продажів за допомогою мобільних пристроїв, таких як смартфони та планшети. Він включає мобільні покупки, банківські послуги та платежі. Мобільні чат-боти полегшують електронну комерцію, дозволяючи споживачам здійснювати транзакції за допомогою голосових або текстових розмов.

У цій сфері було проведено багато досліджень і рекомендовано різні методи, моделі та підходи до безпеки електронної комерції. Загальний консенсус полягає в тому, що безпека електронної комерції включає більше, ніж традиційні п'ять послуг безпеки: ідентифікацію та автентифікацію, авторизацію, цілісність, конфіденційність та неспростування. Безпека електронної комерції повинна враховувати як технічні, так і бізнес-ризики

для того, щоб бути прийнятою. Крім того, вона повинна бути інтегрована в стратегію електронної комерції оскільки вона є допоміжним засобом, а не просто доповненням до неї. Порівнюючи вимоги до безпеки для електронної комерції з вимогами безпеки у фізичному світі, стає зрозуміло, що необхідно задовольнити додаткові вимоги.

У фізичному світі споживач, входячи в бізнес, одразу ж приймає рішення про рівень довіри, який він буде надавати транзакційним можливостям організації. Якщо це добре відомий бізнес, який існує вже деякий час, то довірчі відносини були б побудовані, і споживач не вагався б при здійсненні транзакцій. Довіра ще більше підвищується завдяки фізичній присутності бізнесу. Споживач майже не боїться, що бізнес зникне за одну ніч безслідно. Спілкування з людьми віч-на-віч також підвищує рівень довіри. Більшість споживачів також довіряють процесу здійснення операцій фізичними особами, оскільки відповідно до законодавства вони повинні регулярно перевірятися аудиторами. Хоча порушення все ще можуть прослизнути, більшість людей відчувають себе в безпеці, укладаючи угоди з фізичними особами транзакції. Використання кредитних карток як способу оплати в ресторанах, магазинах одягу та супермаркетах є звичним явищем для більшості людей.

У сфері e-commerce всі вищезазначені вимоги ставляться під сумнів. Багато нових ініціатив у сфері електронної комерції з'являються за одну ніч, і багато з них закриваються так само швидко.

Відсутність довіри до інтернет-підприємств не є безпідставною, оскільки існують численні історії про викрадені номери кредитних карток, невиконані закупівлі та незадовільних товарів та послуг. Немає фізичної присутності, немає реальних людей, і, найголовніше, немає способу визначити, якими є транзакційні можливості веб-підприємства. Тому організації, які бажають брати участь в електронній комерції, повинні зосередитися на встановленні довіри. Одним з механізмів для цього є

інформаційна безпека. Для забезпечення довіри в різних аспектах можуть використовуватися різні механізми та інструменти безпеки, але якщо не буде застосовано цілісного підходу, рівень довіри не буде достатнім для того, щоб клієнти могли брати участь у будь-якій формі транзакцій.

Інший підхід - за допомогою веб-забезпечення. Веб-забезпечення, як правило, означає розгляд питань безпеки, конфіденційності та захисту прав споживачів. Безпека відноситься до необхідних технологій для захисту транзакцій, конфіденційність - до способу зберігання та використання особистої інформації, а захист прав споживачів - це запевнення клієнта в тому, що процеси транзакцій є правильними і що споживач має певні засоби правового захисту у випадку незадовільної транзакції.

На рисунку 1.1 проілюстровано компоненти, з яких складається забезпечення безпеки електроної комерції.

Рисунок 1.1 – Компоненти веб-забезпечення

У сфері ЕК організація повинна мати можливість здійснювати транзакції 24 години на добу, 7 днів на тиждень. Планування безперервності

бізнесу і планування відновлення після аварій зазвичай використовуються для цієї з цією метою.

Конфіденційність стосується способи зберігання та пошуку інформації в організації, а також способи її використання.

Захист прав споживачів - це концепція, яка існує і в рамках фізичного бізнесу. Основною метою захисту прав споживачів є забезпечення того, щоб бізнес вівся справедливо по відношенню до всіх залучених сторін.

1.2 Загальна характеристика методів управління ризиками безпеки

Електронна комерція відноситься до всіх видів електронних транзакцій між сторонами, незалежно від того, чи є вони фінансовими транзакціями або нефінансовими обмінами інформацією чи іншими послугами [8]. Такий обмін інформацією відбувається між споживачем, бізнесом та/або урядом залежно від типу електронної комерції [8, 9]. Система електронної комерції складається з компонентів (програмне забезпечення, апаратні засоби, процеси, послуги та взаємодія з системами третіх сторін), які здійснюють генерування, розповсюдження та маніпулювання фінансовою інформацією з метою забезпечення комерційних транзакцій та послуг через мережу Інтернет. Така інформація включає фінансову інформацію, інформацію про продукти, клієнтів або замовлення, що забезпечує основні процеси системи [8,9].

Індустрія електронної комерції за останні роки зазнала низки серйозних порушень безпеки, про що свідчать такі атаки, як Target атака в 2013 році та атака на Ebay в 2014 році, в результаті яких постраждали мільйони облікових записів, що зробило їх найбільшими інцидентами кіберзлочинності за обидва роки. У 2018 році низка сайтів електронної комерції, включаючи великих

рітейлерів таких як Adidas (2018) та Macy's Inc. (2018), зазнали порушень безпеки своїх сайтів електронної комерції [10]. Для запобігання таких порушень безпеки здійснюється аналіз загроз безпеки та управління ризиками безпеки [11]. Аналіз загроз безпеці спрямований на загрози системам, які використовують наявні вразливості, щоб завдати зловмисного впливу. Ці загрози безпеці викликають ризики безпеки в системі та потребують управління.

Підхід, орієнтований на загрози, використовує аналіз загроз безпеці для підтримки обраного методу управління ризиками безпеки [12]. Ця комбінація створює ітеративний підхід, орієнтований на загрози, що виробляє (активи, ризики, обробку ризиків та оцінку ризиків) компоненти, важливі для безпеки управління ризиками в системах електронної комерції.

Підходи до управління ризиками безпеки розроблені на основі низки загальних стандартів [13] і методів в літературі [14-20]. У таблиці 1.2 наведено популярні методи управління безпековими ризиками, які були проаналізовані в дослідженнях. Інші методи управління ризиками безпеки проаналізовано в [14].

Таблиця 1.2 – Методи управління ризиками безпеки

№	Метод	Джерела
1	Управління ризиками безпеки інформаційних систем (ISSRM)	[12]
2	Австрійський посібник з IT-безпеки	[21]
3	IT- Grundschutz	[22]
4	Метод соціотехнічних систем (STS)	[15,23,24]
5	CORAS	[16]
6	Оперативно-критична оцінка загроз, активів та оцінка вразливостей (OCTAVE)	[17]
7	Аналіз та управління ризиками CCTA Метод (CRAMM)	[18]
8	Висловлення потреб та визначення цілей безпеки (EBIOS)	[19]
9	Метод гармонізованого аналізу ризиків (MEHARI)	[20]

Ми обрали чотири методи CORAS [25], OCTAVE [17], ISSRM [12] та Метод STS [23], оскільки вони мають ілюстративні приклади для вирішення питань управління ризиками безпеки в сфері електронної комерції.

Надамо характеристики методів.

Метод CORAS заснований на моделях метод аналізу захисних ризиків критично важливих для безпеки систем, що використовують інструментальну мову моделювання для моделювання ризиків [25]. Метод CORAS складається з восьми кроків:

- підготовка до аналізу;
- презентація цілей замовнику;
- уточнення цільового опису з використанням діаграми активів;
- затвердження цільового опису;
- ідентифікація ризиків за допомогою діаграми загроз;
- оцінка ризиків з використанням діаграми загроз;
- оцінка ризиків з використанням діаграми ризиків;
- обробка ризиків з використанням діаграм обробки.

CORAS вважається актуальним для управління ризиками кібербезпеки в сфері електронної комерції [26, 27].

Метод OCTAVE (Оцінка критичних операційних загроз, метод активів і вразливостей) – це метод стратегічної оцінки та планування безпеки на основі оцінки ризиків управління ризиками [17]. Метод спрямований на вивчення організаційних і технологічних питань, а також на визначення стратегії та плану безпеки організації. Підхід до управління ризиками складається з трьох компонентів:

– визначення сценаріїв розвитку подій та загроз;

– визначення вразливостей основних активів;

– оцінка ризиків та розробка стратегій безпеки.

OCTAVE використовувався для управління ризиками безпеки в сфері електронної комерції, зокрема, пов'язаними з рішеннями для електронних закупівель [28].

Метод ISSRM (управління ризиками безпеки інформаційних систем) та його доменна модель є практико-орієнтованим методологічним інструментом, орієнтованим на підтримку організацій у прийнятті рішень, пов'язаних з безпекою інформаційних систем [12]. Застосування методу ISSRM складається з наступних шести кроків:

– організаційний контекст і ідентифікація активів;

– визначення цілей безпеки (конфіденційність, цілісність і доступність);

– аналіз та оцінка ризиків;

– рішення про обробку ризику;

– визначення вимог безпеки до впровадження;

– засоби контролю безпеки.

Модель предметної області є важливим артефактом методу ISSRM, яка вводить поняття, пов'язані з активами, ризиками та обробкою ризиків. ISSRM може бути використаний для управління ризиками безпеки в домені електронної комерції [29], а також в інших сферах, таких як авіація [11].

Метод STS (Соціально-технічні системи) [15, 23, 24] для аналізу безпеки прагне подолати ризики безпеки шляхом пропонування трирівневої структури аналізу безпеки бізнес-процесів, додатків і фізичної інфраструктури на основі наступних кроків:

– бізнес-рівень аналіз безпеки високорівневих потреб зацікавлених сторін;

– аналіз безпеки рівня додатків для бізнес-цілей з підвищеною безпекою;

– аналіз безпеки фізичного рівня для цілей додатків з посиленою безпекою.

Підхід визначає, уточнює та поширює вимоги високого рівня безпеки на різні рівні соціотехнічних систем. Він був використаний у практичному прикладі електронної комерції для аналізу ризиків безпеки [24].

Описані методи управління ризиками безпеки порівнюються в табл. 1.3 для вибору методу, придатного для аналізу підходу, заснованого на загрозах.

Таблиця 1.3 – Критерії порівняння різних методів управління ризиками безпеки

Критерії	ISSRM	OCTAVE	CORAS	STS
Актив	++	++	++	+-
Ризик	++	+-	+-	+-
Обробка ризиків	++	+-	++	+-
Оцінка ризиків	++	--	++	--

*++ означає повне виконання, +- означає часткове виконання, - - означає невиконання відповідного критерію.

Порівняння полягає у наступному наборі критеріїв, що формують важливі складові процесу управління ризиками безпеки – це актив, ризик, обробка ризику та оцінка ризику.

Актив – це все, що має цінність і сприяє досягненню цілей організації. Критичні активи системи повинні бути ідентифіковані та захищені в рамках процесу управління ризиками безпеки. Метод ISSRM визнає необхідність ідентифікації активу (відповідно до його доменної моделі) та ілюстрації з використанням орієнтованих на ризики безпеки безпечних мов моделювання (наприклад, [30-33]). OCTAVE визнає цю необхідність [17], але дає менше рекомендацій щодо цього процесу, ніж ISSRM. Метод CORAS також включає ідентифікацію та ілюстрацію активів після попередньої підготовки, включаючи цілі клієнта. Нарешті, метод STS визнає ідентифікацію активів,

зосереджуючись на визначенні потреб зацікавлених сторін у безпеці високого рівня [23].

Ідентифікація ризику є ключовим аспектом будь-якої процедури управління ризиками безпеки. Метод ISSRM підтримує аналіз ризиків за допомогою моделі домену. Модель домену аналізує вразливості, щоб вивести загрози та провести аналіз впливу отриманих ризиків, представлених у вигляді звітів про ризики та моделей. OCTAVE визначає сценарії загроз та вразливості активів перед оцінкою ризиків, представляючи ризики у звітах про ризики [17]. CORAS визначає загрози, використовуючи діаграми загроз і виводить оцінки ризиків з діаграм ризиків. Метод STS підтримує моделювання загроз на основі похідних потреб безпеки, з припущення, що загрози використовують (соціальну або технічну) вразливість [23].

Обробка ризиків. Для управління ризиками, кожен ідентифікований ризик повинен пройти через процедуру обробки ризиків. Ця процедура визнається всіма чотирма вищезгаданими методами управління ризиками, але в різній мірі. Метод ISSRM не тільки розглядає рішення щодо ризику, яке має бути прийняте, але й розглядає реалізацію контрзаходів для зменшення ризиків [12]. CORAS використовує діаграми обробки для ілюстрації діяльності з обробки ризиків. OCTAVE впроваджує стратегії безпеки для боротьби з ризиками безпеки [17]. Метод STS аналізує вимоги безпеки та вибір заходів контролю/контрзаходів для зменшення ризиків [23].

Оцінка ризиків в управлінні ризиками дозволяє зацікавленим сторонам приймати рішення щодо зниження ризиків. Оскільки наявних ресурсів може бути недостатньо для одночасної обробки ризиків, оцінка витрат і вигод є корисною для прийняття рішення про те, які ризики слід обробляти в першу чергу. Метод ISSRM надає можливість оцінити співвідношення витрат і вигод для лікування ризиків [12]. CORAS надає певний аналіз витрат і вигод та оцінки на основі цих діаграм ризиків для обробки ризиків. OCTAVE та STS не надають конкретних оцінок щодо управління ризиками [17, 23].

На основі аналізу можна вважати, що ISSRM відповідає всім розглянутим критеріям з повним задоволенням і, таким чином, будемо використовувати його як основу для нашого дослідження.

Управління ризиками безпеки інформаційних систем (ISSRM)

Модель предметної області [12] (рис. 1.2) для управління ризиками інформаційної безпеки складається з трьох основних груп концепцій: концепції, пов'язані з активами, концепції, пов'язані з ризиками, та концепції, пов'язані з обробкою ризиків.

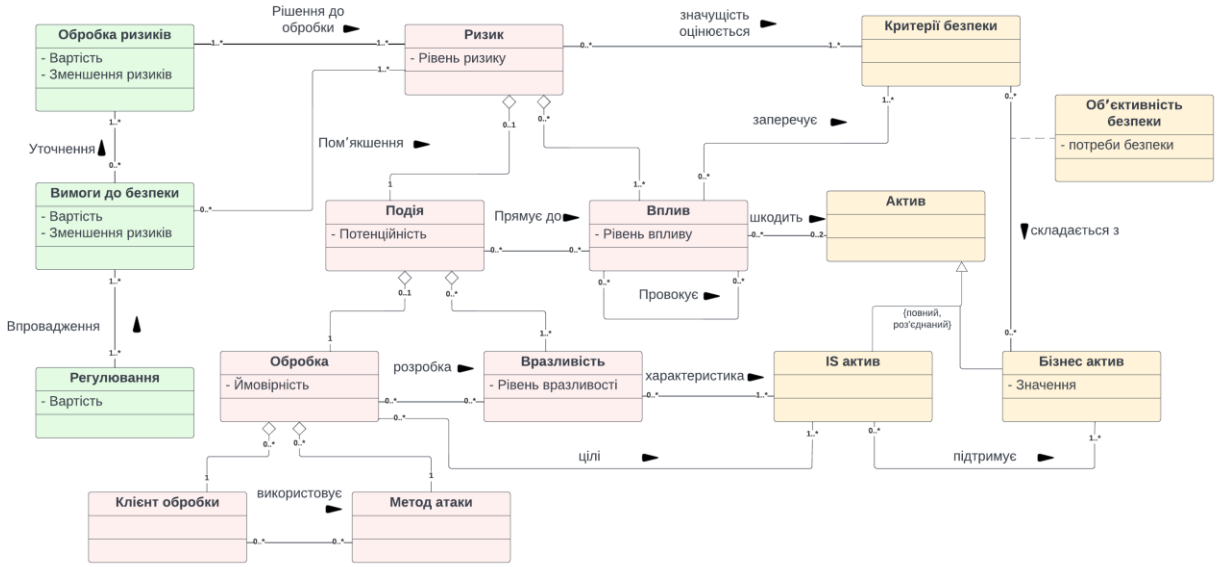

Рисунок 1.2 – Модель домену ISSRM

Концепції, пов'язані з активами, описують системні активи та бізнес-активи для захисту та критерії безпеки для гарантування певного рівня захищеності активів. Бізнес-актив визначається як інформація, дані та процеси, які приносять цінність організації. Системні/Інформаційні активи - це активи, які підтримують бізнес-активи. Критерії безпеки (конфіденційності, цілісності та доступності) є обмеженнями для бізнес-активів, які визначають потреби в безпеці, представлені зацікавленими сторонами.

Концепції, пов'язані з ризиками, містять визначення ризиків та їх складові (загрози, вразливість, подія та вплив). Ризик безпеки - це поєднання

події безпеки та її впливу (заперечення критерію безпеки), що завдає шкоди бізнесу та активам IS. Подія виникає, коли загроза використовує існуючу вразливість. Вразливість - це характеристика активів системи, що є її слабким місцем. Загроза націлена на активи системи, використовуючи їх вразливість.

Концепції, пов'язані з управлінням ризиками, відображають концепції управління ризиками. Рішення щодо обробки ризиків можуть включати зменшення ризику, уникнення ризику, передачу ризику або прийняття ризику. Вимоги безпеки визначають умови, які мають бути досягнуті шляхом зменшення виявлених ризиків безпеки, а засоби контролю реалізують визначені вимоги безпеки. ISSRM також пропонує використовувати метрики в оцінці ризиків для прийняття рішень щодо обробки ризиків. Оцінки ризиків можуть бути отримані на основі бізнес-активів, значень загроз та вразливостей, зниження ризиків та витрат на протидію зниження ризику та вартості контрзаходів [12].

Хоча ISSRM не визначає конкретну мову для застосування в процесі (див. рис. 1.3), його перевага полягає в тому, що він є гнучким до орієнтованих на безпеку мов моделювання [30-33].

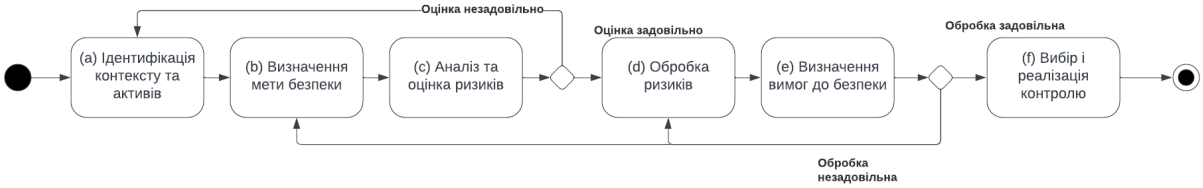

Рисунок 1.3 – Процес ISSRM [11,12]

Методи аналізу загроз безпеки.

Нижче надаємо огляд різних методів аналізу загроз безпеці [34-38].

STRIDE розшифровується як:

– Spoofing - видавати себе за того, ким ти не є, або за того, ким ви не є;

– Tampering (фальсіфікація) - модифікація того, що ви не повинні модифікувати;

– Repudiation (відмова) - твердження, що ви чогось не робили (незалежно від того, правда це чи ні);

– Information disclosure (розкриття інформації) - розкриття інформації тим, хто не має права на її перегляд;

– Denial of service (відмова в обслуговуванні) - атаки, спрямовані на те, щоб переглядати її, які призначені для того, щоб перешкодити системі надавати передбачувану послугу;

– Elevation of privilege (підвищення привілеїв) - коли програма або користувач можуть робити речі (технічно), які вони не повинні робити. Це призначено для того, щоб допомогти розробникам програмного забезпечення ідентифікувати атаки на програмне забезпечення. Кожен з вищезгаданих розділів, присвячений конкретній загрозі, надає більш глибоке пояснення загрози, включаючи її порушення вимог безпеки.

Випадки нецільового використання або зловживання [32] – це випадки, в яких основна увага приділяється діям зловмисника. Випадки нецільового використання мають текстове представлення та діаграми для виявлення загроз безпеки, але вони не надають методичних вказівок для виявлення додаткових загроз і зосередження уваги на загрозах на рівні користувача та організації [32,39].

Дерева атак забезпечують формальний і методичний спосіб опису безпеки системи, заснованої на різних атаках, які можуть статися. Використовується деревоподібна структура представлення атак на систему. По-перше, визначаються цілі атаки. Кожна мета утворює дерево і представляється в кореневому вузлі. Потім формуються всі можливі атаки на кожну ціль і багаторазово додаються вниз по дереву як підцілі, представлені у вигляді листкових вузлів. Дочірні вузли кожного листа представляють шляхи досягнення витісняючої підцілі. Методом моделювання потенційних

шляхів атаки є використання Байєсівських мереж (Bayesian networks). Цей підхід дозволяє будувати дерева атак шляхом перерахування всіх потенційних шляхів атак, забезпечуючи тим самим більш компактне представлення шляхів атак, ніж традиційні методи [40].

Бібліотеки атак надають більш детальний перелік поширених проблем. Бібліотека може бути створена шляхом збору наборів інструментів атаки; або код підтвердження концепції повністю розробленого і/або озброєного коду експлойтів, який допомагає зрозуміти суть атаки. У таких колекціях відсутні будь-які міркування щодо моделювання або абстрагування. Будь-який експерт з безпеки, що використовує бібліотеку атак, повинен витрачати ресурси на створення моделі з атак для аналізу. Таким чином, бібліотеки атак забезпечують меншу абстракцію від загроз і більше деталей для аналізу загроз. Дві поширені бібліотеки атак - це бібліотеки MITRE CAPEC [41] (Common Attack Patterns Enumeration and Classification) - високоструктурований набір шаблонів атак, організованих в групи, і OWASP Top Ten [36] - пропонує десять основних ризиків, характерних для веб-додатків, що охоплюють агенти загроз, вектори атак, слабкі місця в системі безпеки, технічні та бізнес-наслідки.

Шаблони загроз безпеки слідують моделям безпеки [42] для опису конкретних повторюваних загроз безпеці в конкретному контексті безпеки для класифікації широкого спектру загроз. Двома прикладами моделей загроз безпеки є таксономія загроз безпеки для розподілених систем [43] та ризик-орієнтовані моделі безпеки (SRP) [38]. Таксономія загроз безпеки для розподілених систем складається з восьми класів. (атаки на ідентифікаційні дані, атаки на мережеві комунікації, атаки на мережеві протоколи, атаки на передачу нелегальних даних, атаки на збережені дані, віддалений вивід інформації, втрата облікових даних, втрата звітності, неконтрольовані операції) та чотирьох класів загроз безпеці інфраструктури системи (криптографічні атаки, атаки на протидію, атаки на

конфігурацію/адміністрування та атаки на мережеві протоколи) [43]. Моделі, орієнтовані на ризики безпеки (SRP), базуються на розумінні ризиків безпеки (тобто повторюваних проблем безпеки), які виникають в рамках бізнес-процесів (тобто конкретного контексту безпеки) [38]. Моделі, орієнтовані на ризики безпеки характеризуються 5 моделями, які захищають дані від несанкціонованого доступу, передачу даних між суб'єктами господарювання, бізнес-активність після передачі даних, бізнес-сервісів від розподілених атак типу «відмова в обслуговуванні» (DDoS), а також зберігання даних та отримання даних зі сховища.

Ми порівняли описані методи аналізу загроз безпеці, щоб вибрати метод, який підходить для підходу, орієнтованого на загрози. Порівняння проводилося за набором критеріїв, необхідних для повної підтримки процесу управління ризиками – категоризація загроз, потреба в безпеці та пропозиція контрзаходів.

Бібліотеки атак – це колекція типів атак, кожна бібліотека пропонує певну пропозицію щодо протидії виявленій загрозі, але без абстрагування/категоризації або міркувань щодо потреб безпеки. Дерева атак будують атаки на основі цілей ілюструють потреби в безпеці активів в аналізі, але не враховують категоризацію загроз або пропозиції щодо протидії загрозам. Моделі безпеки надають повторювані моделі, виражають потребу в безпеці активів під час аналізу та надають деякі пропозиції щодо контрзаходів для виявленої загрози безпеці, але не надають категоризації загроз безпеці. Однак, система STRIDE дозволяє класифікувати загрози за категоріями в рамках своєї мнемоніки, ілюструє потребу в захисті активів під час аналізу, і може запропонувати контрзаходи в рамках аналізу своєї мнемоніки.

STRIDE відповідає цим вимогам з можливістю доповнення сильні сторони аналізу інших загроз безпеці.

STRIDE - це метод промислового рівня, який використовується для виявлення та аналізу сценаріїв загроз [44]. Для цього дослідження STRIDE був обраний в якості методу аналізу загроз безпеці, який буде використовуватися в подальшому в цій роботі через його галузеве використання, його зрілість, а також високу концентрацію досліджень і використання в спільноті безпеки, що робить його корисним для управління ризиками безпеки. STRIDE дозволяє моделювати та міркувати абстрактно аналізувати елементи системи, такі як потоки даних, сховища даних, процеси та зовнішні сутності, (користувачі, зовнішні сервіси тощо). Класифікація загроз STRIDE визначає типи загроз безпеці в межах представлених елементів. Абревіатура STRIDE - підробка, фальсифікація, відмова, розкриття інформації, відмова в обслуговуванні та підвищення привілеїв формує таксономію. Ці загрози є запереченням основних властивостей безпеки, якими повинна володіти система. Це:

– підробка – аутентифікація;
– фальсифікація – цілісність;
– відмова – невідмова;
– розкриття інформації – конфіденційність;
– відмова в обслуговуванні – доступність;
– підвищення привілеїв – авторизація.

Кожному елементу в рамках представлення системи присвоюється набір сприйнятливих загроз в рамках таксономії STRIDE. Потрібен більш глибокий аналіз, щоб визначити, які загрози в рамках STRIDE застосовні до конкретної системи. Поряд з перевагами в промисловій практиці, STRIDE має головну перевагу - широку, багаторазову базу знань в рамках своєї класифікації.

Підхід на основі загроз.

Підхід, орієнтований на загрози, зосереджується на виявленні загроз безпеці, розподілі зусиль для захисту активів від загроз безпеці та ризиків,

що виникають внаслідок цього, а також на розумінні методів підтримки цих зусиль. Загрози можуть завдати шкоди інформаційним системам та організаційним активам, а отже, повинні бути основною рушійною силою добре спроектованої та адекватно захищеної інформаційної системи. Підходи, орієнтовані на загрози, були використані в дослідженнях [45-47] для моделювання, перевірки та захисту програмних додатків. Підхід, заснований на загрозах, запропонований в цій дослідницькій роботі, передбачає використання STRIDE для підтримки зусиль ISSRM, щоб таким чином забезпечити всебічне бачення ландшафту загроз при управлінні ризиками, що виникають в результаті цього. Наведемо причини такого поєднання.

Моделювання загроз. Застосування STRIDE підтримує ідентифікацію загроз для концепцій, пов'язаних з активами. Наприклад, дослідження BPMN-моделі системи (що ілюструє її активи) може дозволити аналітикам виявити випадки, коли відбувається підміна для здійснення зловмисної дії, або де дані чи код можуть бути модифіковані (тамперінг) для перешкоджання досягненню бізнес-цілей. Застосування STRIDE для ідентифікації загроз як повідомляється, є простим у використанні, дозволяє отримати значну кількість загроз для аналізу [48]. Ідентифікація загроз не суперечить визначенням загроз за методом ISSRM, оскільки ці загрози можуть бути пов'язані з потенційним зловмисником, мотивом та дією загрози, а також уразливістю в цій системі, яка створює життєздатну загрозу. Цей метод є ітеративним і може повторюватися для отримання правильно визначених загроз безпеці.

Категоризація загроз. STRIDE дозволяє класифікувати ідентифіковані загрози під кожною частиною своєї мнемоніки. Ця категоризація стає можливою завдяки її чітким частинам, які належним чином відрізняють одну категорію від іншої за визначенням та за її мнемонічними символами.

Вираження потреб у безпеці. Кожна конструкція STRIDE представляє протилежність деяким типам властивостей безпеки, які повинна мати система, а саме: конфіденційність, цілісність, доступність, аутентифікація, авторизація та невідмова. При розгляданні впливу ризиків, що виникають в результаті, ці впливи зводять нанівець критерії безпеки, а саме прямі обмеження потреб організації у сфері безпеки. Ідентифікація та пом'якшення ризиків в рамках конструкцій STRIDE є ще одним кроком на шляху до досягнення потреб безпеки системи. Наприклад, усунення ризику розголошення інформації наближає організацію на крок до досягнення конфіденційності її активів.

Висловлення вимог до безпеки. Вимоги безпеки включають в себе умови, які необхідно виконати для зменшення ризиків та забезпечення безпеки системи та її бізнес-активів. STRIDE дозволяє визначити вимоги безпеки щодо аутентифікації, цілісності, невідмови, конфіденційності, доступності та авторизації, і все це в рамках конструкцій STRIDE. Наприклад, загрози несанкціонованого втручання можуть слугувати основою для визначення вимог до безпеки авторизації, таких як «додаток повинен робити та зберігати записи інформації, захищені від несанкціонованого втручання».

Пропозиція щодо контрзаходів. Оскільки кожен сценарій STRIDE передбачає вимоги до безпеки в системі, ці вимоги можуть бути використані для того, щоб запропонувати можливі контрзаходи для зменшення ризиків. Наприклад, у випадку загрози підвищення привілеїв, коли авторизація є важливою властивістю безпеки, пропозиції щодо контрзаходів, такі як впровадження RBAC (контроль доступу на основі ролей), DAC (дискреційний контроль доступу), MAC (контроль доступу до носія), UAC (контроль облікових записів користувачів) і захист привілейованих облікових записів [49] можуть бути запропоновані для зменшення ризику безпеки.

У дослідженнях існують споріднені підходи щодо використання методів аналізу загроз та управління ризиками для захисту інформаційних систем [50-51]. Наразі ми розглянемо дослідження щодо окремого використання методу аналізу загроз, комбінації методів аналізу загроз та поєднання методу аналізу загроз з методом управління ризиками безпеки.

Дослідники використовували STRIDE для аналізу загроз для систем телемедицини [17] і загальних хмарних веб-додатків для аналізу потенційних загроз і забезпечення безпеки цих інформаційних систем. Xin and Xiaofang використовують STRIDE у поєднанні з аналізом дерева загроз для аналізу та оцінки безпеки системи інтернет-банкінгу [50]. Однак, в цих дослідженнях не розглядається, як управляти виявленими загрозами безпеки.

Поєднання аналізу загроз з методами управління ризиками безпеки забезпечує ітеративне виявлення та зменшення ризиків безпеки інформаційних систем. Одним з прикладів є поєднання методу аналізу загроз Security Risk Oriented Patterns (SRP) та управління ризиками безпеки ISSRM для розробки безпечної системи в авіаційно-обслуговуючому комплексі. Ці моделі виявляють ризики для безпеки в бізнес-процесах системи та надають пропозиції щодо пом'якшення наслідків для моделей ризиків. Однак використання SRP не позбавлене обмежень. SRPs обмежені бізнес-процесом системи. Таким чином, системні активи, які не представлені в бізнес-процесі не розглядаються для аналізу потенційних загроз та ризиків. Крім того, загрози безпеці, які можуть бути похідними від бізнес-процесу, можуть не охоплюватися цими 5 моделями.

Запропонована комбінація STRIDE та ISSRM надасть більше переваг для аналізу загроз безпеці, в тому числі охоплення активів і загроз за допомогою STRIDE. Вона також забезпечує управління ризиками, що виникають внаслідок цього, за допомогою ISSRM. Поки що існує обмежене розуміння того, як STRIDE та ISSRM можуть бути поєднані для здійснення

процедури управління ризиками безпеки. У цій роботі поєднання цих методів застосовується на прикладі електронної комерції.

Висновки до першого розділу

Ми порівняли описані методи аналізу загроз безпеці, щоб вибрати метод, який підходить для підходу, орієнтованого на загрози. Порівняння проводилося за набором критеріїв, необхідних для повної підтримки процесу управління ризиками - категоризація загроз, потреба в безпеці та пропозиція контрзаходів.

2 АНАЛІЗ ТА ТЕНДЕНЦІЇ РОЗВИТКУ E-COMMERCE

2.1 Характеристика розвитку E-commerce

Починаючи з 2007 року з появою iPhone і до сьогоднішнього дня електронна комерція знову трансформувалася завдяки швидкому розвитку Web 2.0 (набір програм і технологій, які дозволяють створити контент, створений користувачами, наприклад, розміщений в Інтернеті соціальні мережі, блоги, вікі-сторінки, а також веб-сайти та програми для обміну відео та фотографіями; широке впровадження мобільних пристроїв, таких як смартфони та планшетні комп'ютери; розширення електронної комерції для включення місцевих товарів і послуг; і поява на економіка обслуговування попиту, яку забезпечують мільйони додатків на мобільних пристроях і хмарні обчислення. Цей період можна розглядати як соціологічний, а також як технологічний і бізнес-явище.

Визначальні характеристики цього періоду часто характеризують як «соціальний, мобільний, локальний» онлайн-світ. Розважальний контент став основним джерелом доходів від електронної комерції, а мобільні пристрої стали розважальними центрами, а також пристроями для роздрібної торгівлі товарами та послугами на ходу. Маркетинг змінився завдяки зростаючому використанню соціальних мереж, «сарафанного радіо», вірусного маркетингу та набагато потужніших сховищ даних і аналітичних інструментів для справді особистого маркетингу. Компанії значно розширили свою присутність в Інтернеті, вийшовши за межі статичних веб-сторінок до соціальних мереж, таких як Facebook, Twitter, Pinterest і Instagram, намагаючись оточити онлайн-споживача скоординованими маркетинговими повідомленнями. Ці соціальні мережі мають багато спільних характеристик. По-перше, вони покладаються на контент, створений користувачами. «Звичайні» люди (не лише експерти чи професіонали) створюють, діляться та

транслюють вміст величезній аудиторії. Вони за своєю суттю дуже інтерактивні, створюючи нові можливості для соціального спілкування людей з іншими. Вони залучають надзвичайно велику аудиторію (понад 2 млрд користувачів у всьому світі станом на грудень 2019 року у випадку Facebook). Ці аудиторії надають маркетологам надзвичайні можливості для цільового маркетингу та реклами.

Нещодавно переосмислення електронної комерції призвело до появи ряду компаній, що надають персональні послуги за запитом, таких як Uber, Airbnb, Instacart і Deliveroo. Ці підприємства змогли використати великий резервуар невикористаних активів (автомобілі, вільні кімнати та особистий вільний час) і створити прибуткові ринки на основі інфраструктури мобільної платформи. Кейс Insight on Business , Rocket Internet, розглядає Rocket Internet, який інвестував у низку стартапів і наставницьким ними.

Характеристики періодів розвитку електронної комерції наведені в табл. 2.1.

Таблиця 2.1 – Характеристики періодів розвитку електронної комерції

1995-2000 Створення	2001-2006 Консолідація	2007- сьогодення
1	2	3
Орієнтована на технології	Орієнтована на бізнес	
Акцент на зростання доходів	Акцент на доходах і прибутках	Акцент на зв’язки з аудиторією та соціальними мережами
Венчурне фінансування	Традиційне фінансування	Повернення фінансування венчурного капіталу; викуп стартапів великими фірмами
Некерований	Посилене регулювання та управління	Розширене урядове управління наглядом
Підприємниці	Великі традиційні фірми	Підприємницькі соціальні, мобільні та місцеві фірми
Деінтермедіація	Зміцнення посередників	Поширення невеликих онлайн-посередників, які орендують бізнес-процеси більших фірм

Продовження таблиці 2.1

1	2	3
Ідеальні ринки	Недосконалі ринки, бренди, і недосконалості мережевих ефектів	Продовження недосконалості онлайн-ринку; товарна конкуренція на окремих ринках
Чисті онлайн стратегії	Змішані «цеглини та кліки» стратегії	Повернення чистих онлайн-стратегій на нових ринках стратегій; розширення bricks-and-clicks на традиційних роздрібних ринках
Переваги першого учасника	Сила стратегічного послідовника, додаткові активи	Переваги першопроходців повертаються на нових додаткових ринках активів, коли традиційні веб-гравці наздоганяють згаяне
Товари низької складності в роздріб	Роздрібна торгівля високої складності	Роздрібна торгівля, послуги та контент-продукти та послуги

Особливого зростання електронна комерція набула у 2020 році. У 2020 році електронна торгівля сягнула рекордних 16,4% від усіх світових роздрібних продажів. Найбільше показники зросли у країнах центральної Європи – на 21,5%, в українському рітейлі частка e-Commerce досягла 8,8%. (рис. 2.1).

Зростання цифрової комерції означає постійну зміну того, як люди здійснюють покупки. Насправді галузева модель Morgan Stanley разом з іншими даними свідчить про те, що електронна комерція продовжуватиме набирати обертів навіть у країнах, де онлайн-магазини вже популярні.

У Південній Кореї, завдяки добре розвиненій платіжній та логістичній інфраструктурі, онлайн-продажі вже становлять 37% усієї роздрібної діяльності. Але зростання там не закінчено. Електронна комерція в Південній Кореї може зрости до 45% протягом наступних п’яти років завдяки доставці їжі та варіантам доставки в той же день.

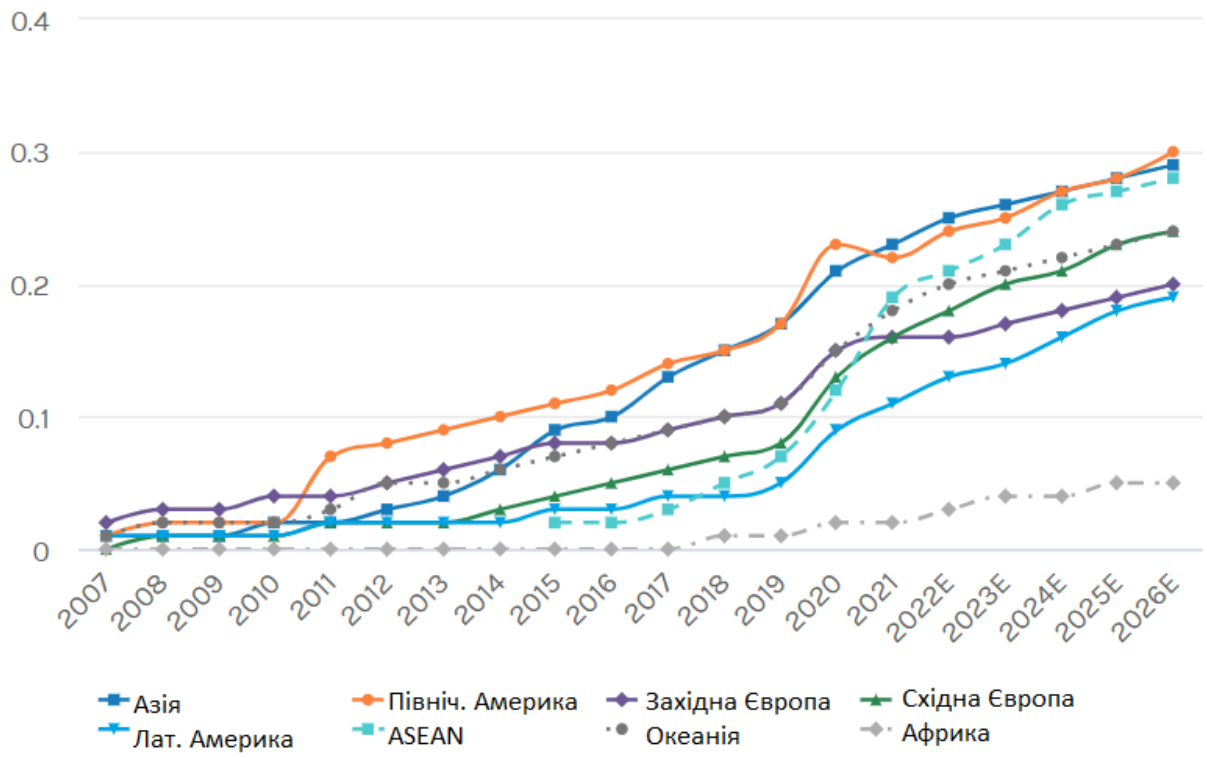

Рисунок 2.1 – Частка електронної комерції в роздрібних продажах продовжує зростати в регіонах

Подібним чином у США електронна комерція може досягти 31% продажів до 2026 року проти 23% зараз, оскільки звичайні магазини закриваються, а споживачі віддають перевагу зручності.

Ринки електронної комерції на ранніх стадіях і нові сегменти також готові до значного зростання. Наприклад, у деяких частинах Південно-Східної Азії та Латинської Америки електронна комерція може зрости на 17% і 20% відповідно протягом наступних п’яти років і щорічно зростати.

Якщо говорити про сегменти, то електроніка, яка лідирує в усіх категоріях електронної комерції, планується збільшити з 38% роздрібних продажів до 45% світових роздрібних продажів. Цифрові продажі також зростають у нових галузях, зокрема в сфері краси, одягу та продуктів.

Використання Інтернету та розширене підключення також є значними рушійними силами, особливо на ринках, що розвиваються, де населення стає молодшим і проводить більше часу в Інтернеті, ніж їхні колеги на

розвинених ринках. Наприклад, споживачі в Колумбії та Бразилії проводять в Інтернеті в середньому більше п’яти годин щодня, створюючи значну можливість для роздрібних торговців вийти на новий ринок клієнтів [52].

2.2 Аналіз постпандемічного стану e-commerce

Зважаючи на наслідки COVID-19 індустрія електронної комерції кардинально змінилася за останні два роки. Це найпомітніші тенденції електронної комерції після COVID (рис. 2.2).

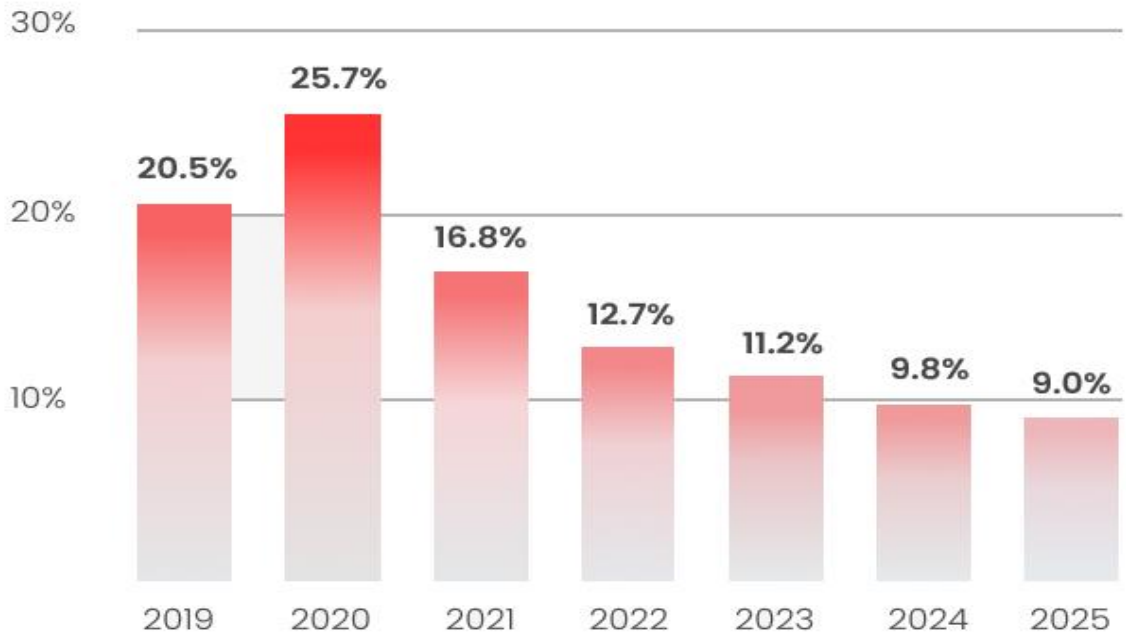

Рисунок 2.2 – Темп зростання електронної комерції

Після стрімкого зростання продажів електронної комерції у 2020 році слід було очікувати уповільнення зростання в 2021 році. Порівняно з 2020 роком, коли продажі електронної комерції зросли на 25,7%, 2021 рік із темпом зростання на 16,8% більш повільний. Однак повільніше зростання

можна пояснити декількома факторами, від повернення покупців до покупок у магазині до проблем із ланцюгом постачання, які обмежували можливості продажів для багатьох компаній електронної комерції.

З початком пандемії в електронній комерції з'явилася нова тенденція: онлайн-шопінг. Одним словом, потенційні покупці все частіше наповнюють свої візки для покупок, а потім залишають їх перед тим, як розрахуватися.

Це, безперечно, почалося як пандемічна тенденція, коли нездатність покупців відвідувати звичайні магазини в поєднанні з тим, що вони застрягли вдома під час карантину, змусила їх шукати заміни своїм звичним звичкам покупок. На початку пандемії було покинуто до 94,4% візків. У середньому до 70% кошиків залишаються на всіх ринках електронної комерції, причому найвищий рівень залишення належить до mCommerce, де 85,65% користувачів заповнюють свої кошики для покупок і ніколи до них не повертаються. Це становить 18 мільярдів доларів втраченого доходу щороку.

Можливими рішеннями цієї проблеми є зміна дизайну кошика для покупок, додавання чітких закликів до дії та надання гостьової оплати. Лише це може підвищити рівень конверсії на 45%.

З березня 2020 року індустрія електронної комерції зіткнулася з багатьма проблемами, включаючи дефіцит товарів і затримки доставки. Однак для більшості покупців важливий лише пункт обслуговування «останньої милі». Покупець, як і раніше, розраховує отримати необхідний товар за адекватною ціною і в розумні терміни. Лише 1 з 5 споживачів у США готовий пробачити постачальникам послуг затримки та інші невідповідності послуг, але є винятки з цієї тенденції — лояльність до бренду робить покупців більш поблажливими навіть у разі ускладнень замовлення.

У постпандемічному ландшафті електронної комерції відбулися зміни в лояльності клієнтів і пріоритетах. Коли клієнт знаходить бренд, який відповідає його очікуванням і етичним принципам, він, швидше за все,

залишиться з ним навіть через затримки доставки та відсутність товару. Крім того, клієнти тепер менш схильні до випадкового вибору бренду для підтримки. Наприклад, для 47% покупців для магазину електронної комерції важливо мати місцеву присутність, тоді як 78% покупців визнали, що частіше роблять покупки в закладах поблизу, щоб підтримати місцеву економіку. А ціна є менш значущим фактором у процесі вибору для багатьох покупців, оскільки 7 із 10 покупців радше підтримають місцевий бізнес, навіть якщо це означає сплатити більше (рис.2.3).

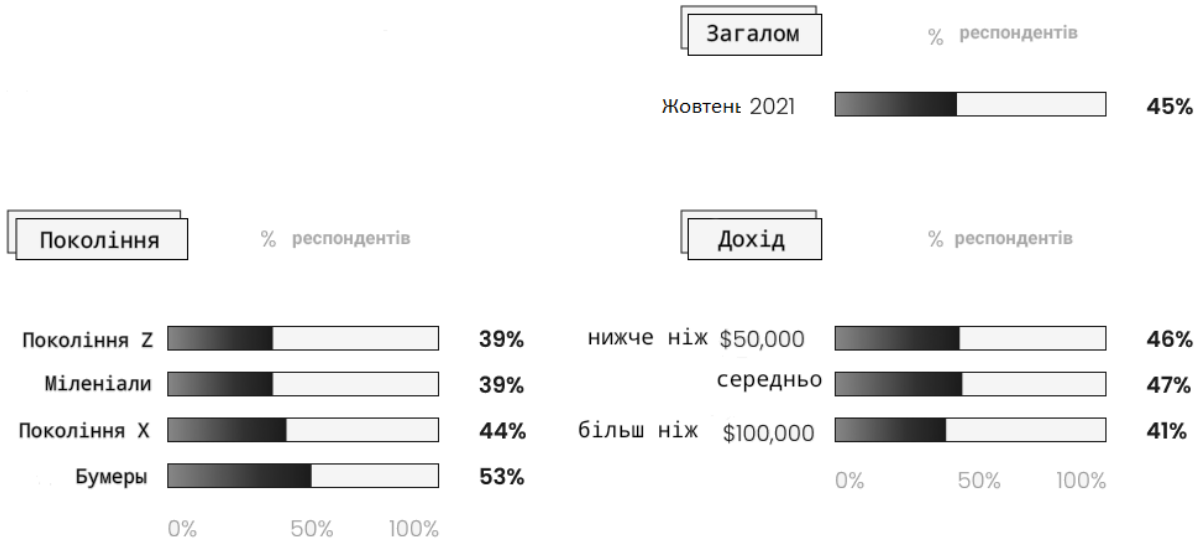

Рисунок 2.3 – Фактори вплаву на покупців в e-commerce

Порівняно з 2020 роком, у 2021 році споживачі повернулися до діяльності поза домом. До жовтня 2021 року близько 50% споживачів у США почали частіше виходити з дому — не лише для покупок, але й для роботи в офісі, насолоджуватися світськими заходами та їсти вдома. З січня 2021 року ця діяльність зросла на 44%.

Коефіцієнт повернення поза домом залежить від кількох факторів, у тому числі покоління, причому бебі-бумери на 14% частіше залишають домівку, ніж покоління Z, а домогосподарства з високим доходом залишаються вдома частіше, ніж сім’ї з низьким і середнім доходом.

Товари з найшвидшим зростанням продажів. За час пандемії різні продукти пройшли через хвилі популярності. Однак деякі продукти користувалися стабільним попитом і добре проявляли себе в продажах протягом цих двох років. Більшість найбільш продаваних товарів можна розділити на три групи:

– здоровий спосіб життя: очищувачі повітря, фільтри для води, паропральні машини;

– робота з дому: ноутбуки, монітори, навушники;

– кулінарія: кухонна техніка, кухонні комбайни, кавоварки (рис 2.4).

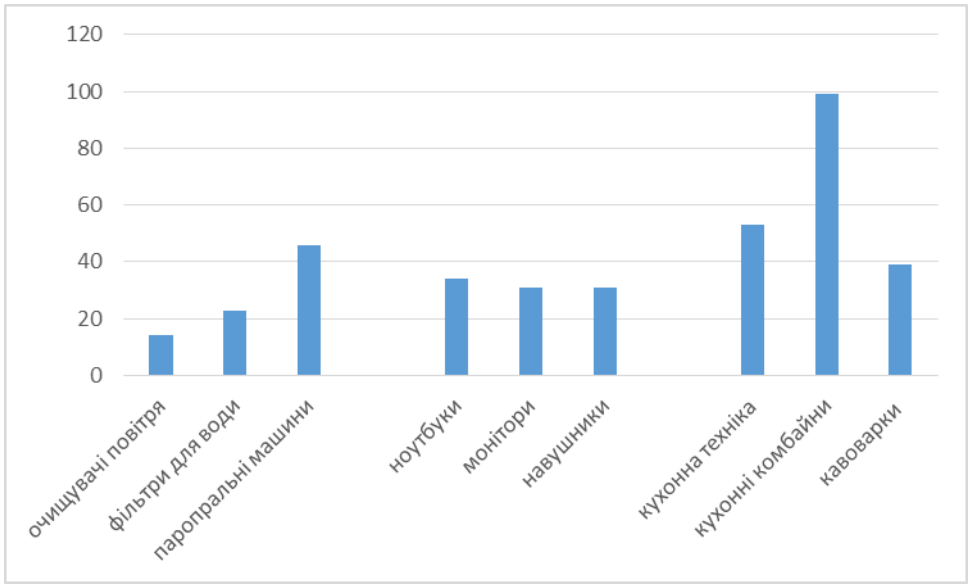

Рисунок 2.4 – Показники зростання окремих товарів у електронній комерції

Після астрономічного зростання 2020 року електронна комерція тепер пристосовується до нової реальності. Оскільки пріоритети клієнтів змінюються, і вони більше усвідомлюють лояльність свого бренду, підприємствам електронної комерції потрібно зміцнити свої позиції на ринку, оскільки споживачі швидко перейдуть до конкурентів, якщо вони не задоволені послугою, яку вони отримують.

Як одна з найбільш швидкозростаючих галузей, електронна комерція регулярно зазнає незначних і серйозних трансформацій, і сезон 2021/2022 не є винятком. Є кілька помітних тенденцій, які дають досить гарне уявлення про те, де зараз знаходиться галузь і куди вона рухається.

Тенденція 1. Криза ланцюга поставок загрожує всій галузі роздрібної торгівлі. У 2020 році затримки доставки та запаси продукції вплинули не тільки на світ електронної комерції, а й на індустрію роздрібної торгівлі в цілому. Це було особливо великою проблемою під час святкового сезону 2020 року, коли мільйони покупців отримали свої замовлення через кілька тижнів після зимових свят, що призвело до величезної низки повернень подарунків, які більше не були потрібні. І це є суттєвим негативним явищем для малого чи середнього бізнесу електронної комерції. Проте ситуація не дуже покращилась і зараз. У 2021 році компанії електронної комерції відчули дефіцит не тільки продукції, яку вони продають, але й пакувальних матеріалів та запасних частин складського обладнання.

Існує кілька причин нинішньої кризи ланцюга поставок, від дефіциту морських контейнерів і більш ніж 500% збільшення витрат на доставку з Китаю до заторів контейнерів у великих портах. Найважливіше – це здатність підприємств електронної комерції швидко адаптуватися до нових умов. Серед іншого, компаніям електронної комерції слід розглянути можливість диверсифікації своєї бази постачальників, щоб уникнути подальших ускладнень та використання технологічних рішень для прийняття рішень на основі даних. Наприклад, інструменти аналізу даних можуть допомогти передбачити попит клієнтів, тим самим допомагаючи зрозуміти, якими товарами запасатися.

Тенденція 2. Омніканальна електронна комерція.

Омніканальна стратегія роздрібної торгівлі – практика створення безперебійного досвіду покупок для покупця по всіх доступних каналах, включаючи електронну комерцію та магазини– не зовсім нова тенденція. Але

з 2020 року вона демонструє значне зростання. Завдяки багатоканальним кампаніям, які забезпечують 287% купівель, омніканальні маркетингові зусилля окупаються. (рис.2.5)

Рисунок 2.5 – Тенденції зміна каналів отримання продукту

За даними Think With Google, хоча кількість людей, які здійснюють покупки в Інтернеті, значно зросла за останні два роки, 66% покупців все ще планують робити покупки в магазині [53]. Більш того, покупець 15 років тому зазвичай проходив через дві точки дотику, щоб купити товар, в той час як сучасний покупець в середньому проходить через шість. Це означає, що кампанії не можуть бути односторонніми і повинні залучати різні види ЗМІ, від соціальних мереж та маркетингу електронною поштою до роздачі листівок.

Тенденція 3. Соціальна електронна комерція відкриває нові можливості. Протягом багатьох років підприємства електронної комерції активно працюють у соціальних мережах. Однак компанії в основному використовували веб-сайти соціальних мереж, щоб дозволити більшій кількості потенційних клієнтів відкривати свої продукти, а не продавати їм

безпосередньо. 70% покупців зараз звертаються до Instagram, щоб спланувати свою наступну покупку.

Звичайно, Instagram - не єдина платформа для проведення кампаній соціальної комерції. Facebook і Pinterest вже розгорнули функції покупок, а YouTube, TikTok і Twitter тестують різні версії кнопок «зробити покупки зараз».

10 категорій електронної комерції в США, які найкраще розвивалися у 2021 році.

- комп'ютерна та побутова електроніка;
- одяг та аксесуари;
- меблі та предмети інтер'єру;
- здоров'я, особистий догляд та краса;
- іграшки та хобі;
- авто і запчастини;
- книги, музика та відео;
- продукти харчування та напої;
- оргтехніка та витратні матеріали;
- інше.

Електронна комерція стрімко розвивається по всьому світу, і саме тут справи стоять на даний момент.

Тенденція 4. Маркетплейси домінують у галузі.

Присутність маркетплейсів на міжнародному ринку електронної комерції сильна, і з кожним роком вона тільки міцніє. У 2021 році 48% успіху онлайн-покупців по всьому світу почали б пошук на одному з популярних маркетплейсів. Зараз у кожній частині світу є ринки та кілька видатних компаній, які працюють у всьому світі. На рис. 2.6 представлено 10 найкращих ринків 2021 року за щомісячними відвідуваннями.

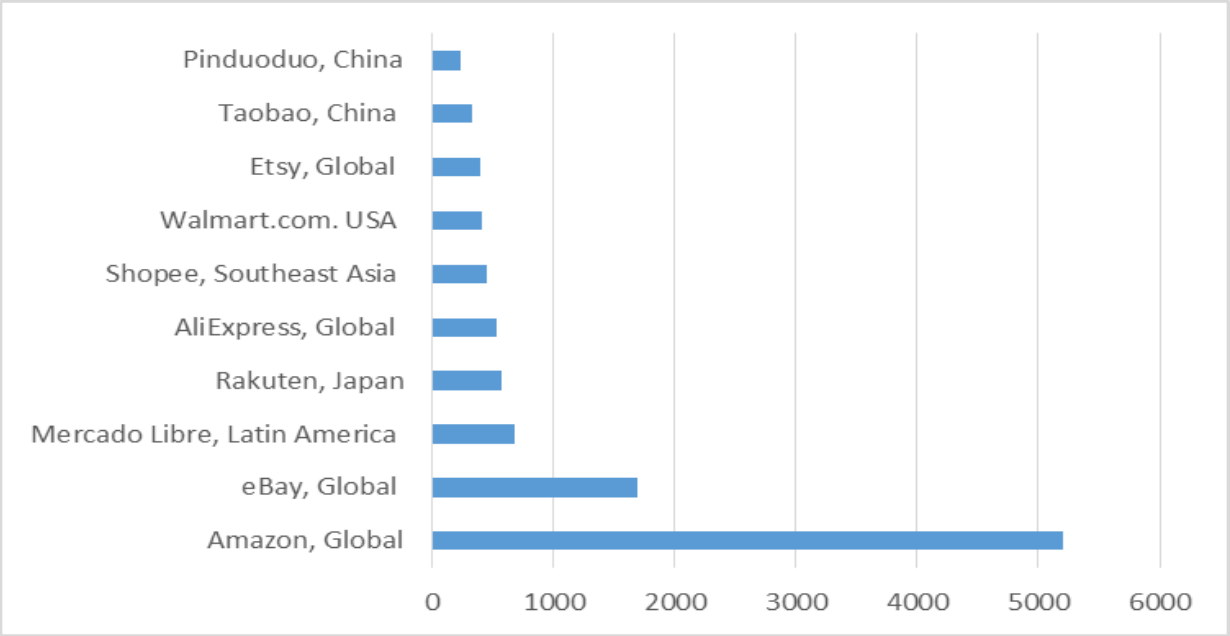

Рисунок 2.6 – Найбільші маркетплейси, млн.візітів/місяць

Джерело [54]

Amazon є одним з провідних гравців на міжнародній арені електронної комерції, і останні два роки тільки зміцнили свої позиції. В даний час він має 13% частки ринку в усьому світі, а в США присутність Amazon є ще більш потужним, оскільки 52% національної діяльності електронної комерції відбувається на цій платформі.

Хоча Amazon залишається силою, з якою слід рахуватися, особливо в західній частині світу, на глобальній карті є райони, де Amazon навіть не знаходиться близько до вершини списку. В Азії та багатьох європейських країнах ці позиції міцно займають азіатські ринки та Alibaba зокрема. Alibaba особливо велика у Східній Європі з часткою ринку 2,9% у 2020 році. А під час Дня холостяка, найбільшої торгової події в Азії, Alibaba та JD.com разом зібрали 139 мільярдів доларів продажів.

З початку 2020 року продажі електронної комерції зросли на всіх регіональних ринках, але деякі продемонстрували ще більше зростання [55]. Безумовним лідером продажів електронної комерції в 2021 році став Китай, досягнувши за обсягами продажів майже в 3,3 рази більше, ніж його

найближчий конкурент – США. Японія, Південна Корея та Індія є трьома іншими азіатськими країнами з топ-10 міжнародних ринків продажів електронної комерції (рис. 2.7).

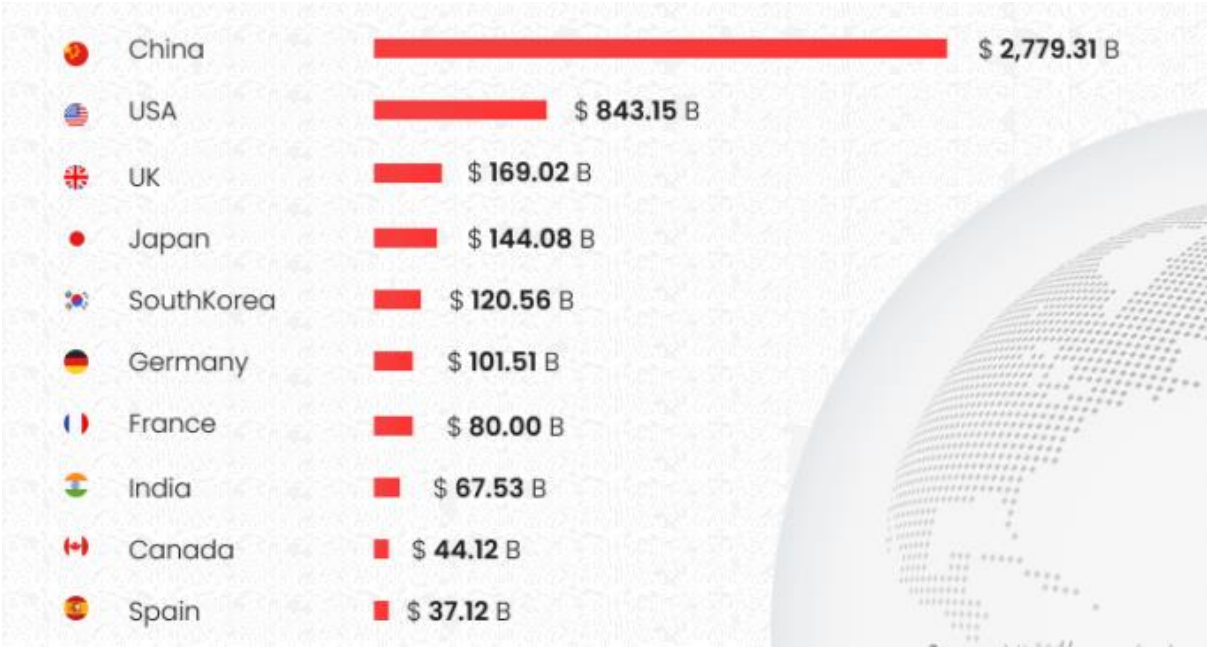

Рисунок 2.7 – Топ 10 найбільших ринків електронної комерції

Природа електронної комерції допомагає зруйнувати бар'єри для міжнародних покупців, але це можливо лише тоді, коли послуга доступна рідною мовою покупця. Згідно з опитуванням [57], 1 з 5 покупців вважає відсутність локалізації великим бар'єром, який може перешкодити їм зробити покупку (рис. 2.8).

Рисунок 2.8 – Відношення покупців до локалізації платформи закупівель *Джерело [57]*

Більше того, оскільки покупці покладаються на відгуки про товари в процесі прийняття рішень, вони також сповнені рішучості знайти відгуки на своїй рідній мові. 66% міжнародних покупців використовуватимуть опцію автоматичного перекладу, якщо вона доступна, але машинний переклад часто може призвести до непорозуміння.

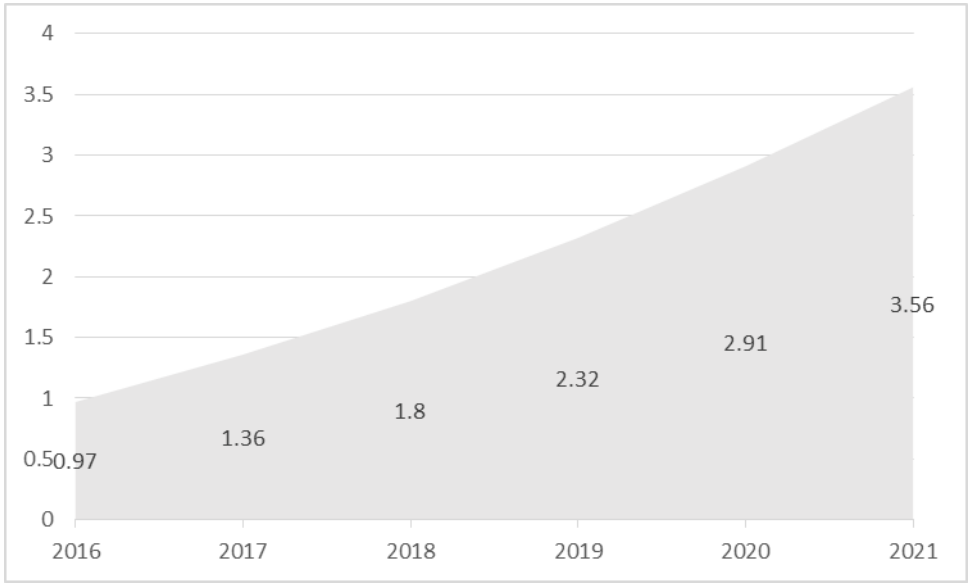

Рисунок 2.9 – Показники зростання mCommerce, трил. дол. США

Тенденції мобільної електронної комерції. З майже 6,4 мільярдами користувачів смартфонів у світі в 2021 році та рівнем проникнення смартфонів від 45% до 95% у різних частинах планети, ринок mCommerce є таким, що швидко зростає.

Ось ключові тенденції mCommerce представлені на рис. 2.10.

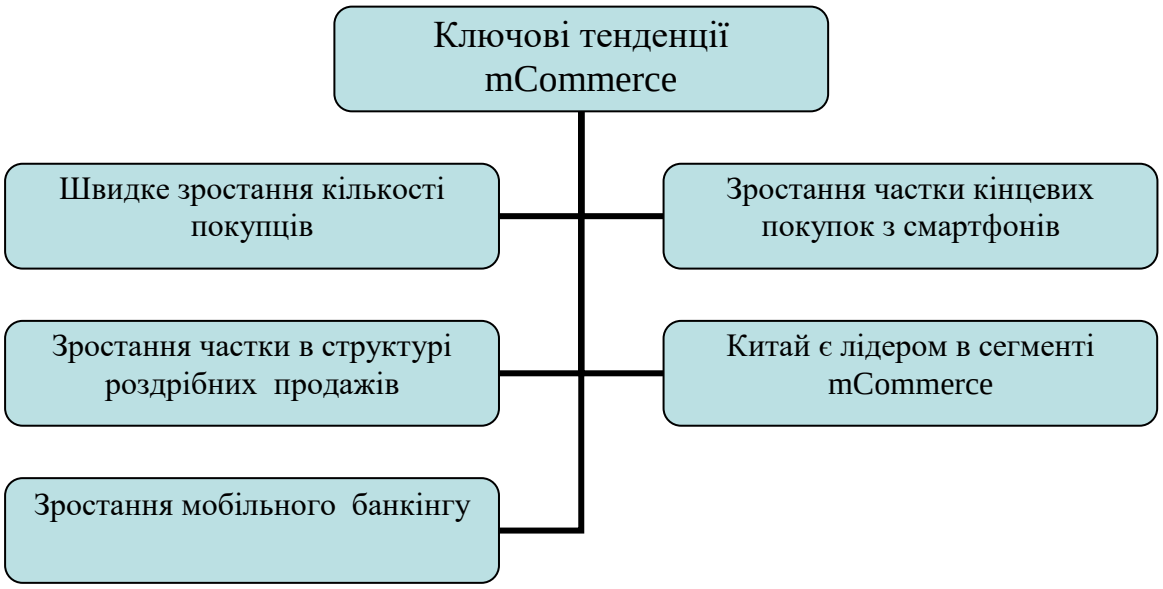

Рисунок 2.10 – Ключові тенденції mCommerce

Продажі mCommerce продовжують неухильно зростати з року в рік. Продажі на ринку мобільної електронної комерції швидко зростають протягом останніх п'яти років, тому зростання не так пов'язане з пандемією, як з рекордно високим рівнем проникнення смартфонів у всьому світі. У 2021 році продажі mCommerce у всьому світі склали $3,56 трлн, і це на 22,3% більше, ніж у 2020 році, коли продажі mCommerce принесли $2,91 трлн.

За оцінками, у світі є 2 мільярди людей, які зробили принаймні одну покупку в Інтернеті. І мобільні продажі не так вже й відстають: 3 з 4 користувачів електронної комерції у всьому світі роблять покупки зі своїх смартфонів. Більше того, багато покупців мобільних пристроїв використовують омніканальну тактику покупок, коли вони переглядають веб-сайт електронної комерції зі свого настільного комп'ютера і в кінцевому

підсумку роблять покупку на мобільному пристрої – 58% усіх покупок на кількох пристроях закриті на мобільних пристроях.

mCommerce продовжує експансію. У 2020 році mCommerce відповідала за 5,5% від загального обсягу роздрібних продажів у США. У 2021 році він зріс до 5,9%. Підраховано, що до 2025 року 10,4% всіх роздрібних продажів в США буде здійснюватися на мобільних пристроях. З постійним поширенням нових технологій mCommerce, таких як AR і 5G, а також популярністю швидких способів оплати, таких як Apple Pay і Google Pay, mCommerce стане ще більш потужною в найближчі роки.

Азія в цілому і Китай зокрема лідирують в сегменті mCommerce. 3 з 5 ринків mCommerce у світі знаходяться в Азії. Китай лідирує в пакеті з продажами mCommerce $750 млрд, Японія займає четверте місце з $34,5 млрд, а Південна Корея займає п'яте місце з ринком mCommerce $28,8 млрд. Азія також лідирує, коли справа доходить до відсотка мобільних транзакцій. З 79,1% транзакцій, що відбуваються на мобільних пристроях в Індонезії, 74,2% в Таїланді та 69,6% на Філіппінах, Азія стає найбільш перспективним ринком mCommerce у всьому світі.

Розширення мобільної комерції неможливо без зміни банківських звичок населення планети. Зокрема, маючи понад 1 мільярд користувачів по всьому світу, мобільний банкінг зараз є однією з найбільш швидкозростаючих технологій, пов'язаних з mCommerce. Для деяких мобільний банкінг просто означає доступ до швидких транзакцій і кращий контроль банківського рахунку. Для інших, особливо в Азії та Африка, мобільний банкінг виступає єдиною формою фінансової інклюзії, коли немає інших варіантів.

Ринок mCommerce розвивається тими ж темпами, що і традиційна електронна комерція, або навіть швидше в певних частинах світу. Кількість власників смартфонів і користувачів mCommerce збільшується з кожним роком. Але досягти успіху на конкурентному ринку мобільної комерції

практично неможливо без використання передових технологій і задоволення конкретних потреб зростаючої аудиторії mCommerce.

Тенденції B2B електронної комерції Сучасні B2B-компанії успішно розширили свою присутність до онлайн-сфери, Нижче наведені найважливіші тенденції зі світу B2B електронної комерції.

B2B маркетплейси покращують свої позиції.

B2B-компанії більше не продають виключно свої товари та послуги через власні веб-сайти. B2B маркетплейси значно зросли за останні кілька років. Ця тенденція розвивається в тому ж дусі, що і традиційні ринки електронної комерції, оскільки все більше і більше постачальників B2B і клієнтів відкривають для себе переваги маркетплейсів.

Simamkele Matuntuta зазначає, що у 2021 році 26% клієнтів B2B здійснюють від 50% до 74% своїх покупок в Інтернеті, а 9% клієнтів роблять понад 75% від загальної кількості покупок B2B на маркетплейсах [58].

B2B-компанії адаптуються до ринку електронної комерції іншими темпами. B2B компанії стикаються з технологічними проблемами. Деякі розробляють фірмові рішення з нуля, а інші намагаються підтримувати та оновлювати свої існуючі рішення. 57% B2B-компаній стикаються з проблемами, пов'язаними з інтеграцією та оновленням своїх застарілих систем.

Крім того, 44% повідомили, що борються з пошуком правильного партнера з рішення, і це можна легко пояснити – багато чого залежить від високоякісної розробки програмного забезпечення для електронної комерції. Тож рішення найняти розробників електронної комерції є одним із найрозумніших, які може прийняти B2B-компанія, яка хоче вийти на ринок електронної комерції.

Віч-на-віч B2B-продажі раніше були єдиним способом ведення бізнесу на цьому конкурентному ринку. Однак очні B2B-операції поступаються місцем віддаленим і самостійним покупкам. На різних етапах B2B покупок

від 22% до 35% B2B-споживачів віддають перевагу цифровому самообслуговуванню, а від 44% до 48% з них хочуть робити речі віддалено. Ця тенденція, принаймні частково, пов'язана з тим, що 73% осіб, які приймають рішення в сегменті B2B, зараз є міленіалами, які більш відкриті для самостійного обслуговування та віддалених операцій порівняно зі старшими поколіннями [58-59].

Тенденції B2B електронної комерції можуть приходити і йти, але контент залишається ключовою частиною успішної маркетингової стратегії для B2B-компанії. Якісний контент часто може бути єдиним, що підштовхує B2B-компанію до успіху і допомагає їй виділитися серед конкурентів. А різні типи контенту можуть ідеально працювати для різних галузей і маркетингових цілей. Зокрема, до найбільш популярних типів контенту, що використовуються підприємствами B2B, відносяться:

– контент у соціальних мережах – 95%;
– дописи в блозі або короткі статті – 89%;
– інформаційні бюлетені електронною поштою – 81%;
– відео – 71%.

Маркетинг електронною поштою залишається особливо важливою частиною маркетингової стратегії B2B, при цьому 79% респондентів стверджують, що електронні бюлетені є найефективнішим інструментом для формування попиту. І незважаючи на все зростання digital-маркетингу, живі події нікуди не діваються: 73% B2B-компаній регулярно організовують особисті заходи для залучення нових клієнтів.

Ринок електронної комерції B2B розвивається так само швидко, як і традиційна електронна комерція, але має власну траєкторію і стикається з унікальними проблемами, включаючи обслуговування та оновлення застарілої системи. Сильна маркетингова кампанія, а також правильний вибір партнерів з розробки програмного забезпечення для електронної комерції можуть суттєво змінити позицію B2B компанії на ринку.

2.3 Характеристика основних загроз безпеці e-commerce

2021 рік приніс серйозні зміни в конфіденційність в Інтернеті та те, як її розглядають. Деякі з цих змін потенційно можуть мати великий вплив на електронну комерцію та маркетинг, а деякі вже змінюють ринок реклами.

Споживачі більш обізнані про використання даних службами електронної комерції. Покупці електронної комерції більше не сліпо довіряють брендам свої особисті дані. Вони хочуть знати, що бренди з цим роблять, і вимагають більш відповідального та прозорого підходу. Зокрема, 61% респондентів, опитаних Shopify, кажуть, що вони поділяться своєю приватною інформацією з брендом лише за потреби, 57% повідомляють про зростаючу стурбованість щодо того, як використовуються їхні дані, а 40% припинили купувати у бренду, коли виникли побоювання щодо використання даних цим брендом [60].

Одна з найбільших змін у конфіденційності даних у 2021 році надійшла від Apple. Компанія представила функцію відмови від відстеження даних в iOS 14.5, і з відтоді все було не так. Бренди отримали набагато менше можливостей для створення цільових пропозицій та залучення нових клієнтів на основі їхньої поведінки. Ця зміна була особливо помітною для Facebook, яка широко використовує дані, зібрані від користувачів, для націлювання на їхню рекламу. У свою чергу, бренди, які часто рекламували через Facebook, в кінцевому підсумку платили вищу ціну за рекламу, яка не приносила очікуваного доходу.

Ще одне оновлення, пов'язане з конфіденційністю, надходить від Google, який у лютому 2020 року оголосив, що збирається поступово відмовитися від сторонніх файлів cookie в Chrome до 2022 року. З тих пір Google переніс дату поетапної відмови на другу половину 2023 року. Google визнає, що конкуренти Chrome можуть продовжувати використовувати

сторонні файли cookie для відстеження активності користувачів, але оскільки понад 65% користувачів у всьому світі використовують Chrome, брендам і рекламодавцям все одно доведеться шукати нові способи охопити свою цільову аудиторію.

Зростаюча обізнаність споживачів про проблеми конфіденційності даних створює додаткові проблеми для підприємств електронної комерції та основних рекламних платформ. Замість того, щоб покладатися на випробувані маркетингові тактики, такі як відстеження поведінки користувачів в Інтернеті, компаніям доведеться проявити більш креативність при націлюванні на свої пропозиції.

Електронна комерція є однією з галузей, які розвиваються на випередження, а не просто реагують на зміни. Щороку приносить багато інновацій у цій галузі, а 2022 рік також пропонує нові способи виділитися на конкурентному ринку електронної комерції.

Розмовний інтернет-шопінг. Оскільки все більше споживачів вимагають зручності покупок та персоналізації, розмовні покупки в Інтернеті можуть стати рішенням, яке шукають підприємства електронної комерції. Сюди входять чат-боти, як такі, як Facebook Messenger, так і віджети чату в реальному часі на платформах електронної комерції, а також програми для голосових покупок, які працюють подібно до Alexa та Siri та допомагають брендам ефективніше звертатися до клієнтів. Голосовий шопінг є особливо перспективною технологією, оскільки очікується, що продажі голосових покупок досягнуть 19.4 мільярда доларів до 2023 року [61].

Оскільки обмеження, пов'язані з COVID, поступово скасовуються, покупці повертаються до магазинів. Однак вони не готові просто так від нього відмовитися. Ось чому реклама місцевого інвентарю, розгорнута Google, була зустрінута з хвилюванням магазинами електронної комерції. Ці оголошення доступні в США, Великобританії, Австралії, Новій Зеландії, Бразилії та Західній Європі. Вони дозволяють магазинам рекламувати свої

запаси, залучаючи більше клієнтів до фізичних магазинів і підвищуючи впізнаваність бренду.

Щоб бізнес електронної комерції випередив конкурентів, він повинен мати унікальну торгову пропозицію. І коли магазин електронної комерції продає той самий продукт, що й десятки інших магазинів, виділитися може бути складно. Персоналізований досвід покупок може бути найкращим виходом щодо персони покупця.

Згідно з дослідженням, 80% покупців очікують персоналізованого досвіду покупок [58]. При чому враховується весь досвід покупця. Бізнесу електронної комерції потрібно використовувати кілька типів даних для задоволення потреб покупців та підвищення їх лояльності.

Традиційно рішення для електронної комерції розробляються в цілому: frontend і backend програми глибоко переплітаються, що іноді ставить завдання при роботі з незвичайними платформами або коли потрібні швидкі оновлення. Ось чому архітектура безголової електронної комерції зараз швидко переймається різними компаніями. Під архітектурою електронної комерції headless backend програми розробляється незалежно від frontend. В результаті контент програми може відображатися не тільки на невеликому спектрі пристроїв, таких як настільні комп'ютери і смартфони, але і на будь-якому типі екрану, який є. Це досягається за рахунок використання API. Електронна комерція без голови - це саме те, що потрібно компаніям в епоху IoT.

Незважаючи на всі технологічні досягнення, існує значний розрив у досвіді покупок при покупці офлайн та онлайн. Доповнена реальність в електронній комерції покликана подолати цю прогалину. При правильному використанні доповнена реальність може допомогти бренду електронної комерції досягти більш високої лояльності клієнтів, підвищити коефіцієнт конверсії та знизити коефіцієнт прибутковості. Деякі з прикладів доповненої реальності, яка використовується в електронній комерції, включають:

– віртуальні примірочні;

– побачивши, як меблі та предмети декору можуть виглядати в домашніх умовах;

– пробуємо різні кольори фарби для стін;

– тестування різних кольорів волосся і макіяжу;

– створення інтерактивних посібників користувача.

Прямі покупки в прямому ефірі - це тип електронної комерції, де товари, рекламовані на відео, продаються в режимі реального часу. Найпоширенішим прикладом покупок у прямому ефірі є випадки, коли впливові особи в соціальних мережах переглядають свої улюблені продукти в Інтернеті, і є посилання або кнопка, де ви можете придбати ці продукти. Прямі трансляції покупок роблять бренди на крок ближчими до своїх клієнтів і допомагають їм охопити конкретний тип аудиторії, який добре реагує на маркетинг впливу.

Динамічне ціноутворення - це не абсолютно нове поняття. Пристосування цін до змін попиту і пропозиції існує вже багато століть. Однак доступ до абсолютно нових технологій допомагає компаніям електронної комерції надалі використовувати динамічне ціноутворення на свою користь. У наші дні бізнес електронної комерції може змінювати ціни на хвилинній основі, використовуючи різні фактори:

– попит і пропозиція;

– рівень запасів;

– тенденції ринку;

– очікування споживачів;

– поведінка споживачів, наприклад, на веб-сайті;

– безпосередня конкуренція.

Потім, на основі даних, отриманих по різних каналах, інтернет-магазин може використовувати інструменти автоматизації управління цінами для вибору найбільш підходящих цін для кожного товару. Найбільшою

перевагою використання динамічного ціноутворення є можливість максимізувати прибуток на кожному проданому товарі.

Сучасні технології відкривають безмежні можливості для бізнесу електронної комерції. Від створення цінової стратегії та підвищення гнучкості існуючого рішення для електронної комерції за допомогою безголової електронної комерції до більш ефективного охоплення цільової аудиторії за допомогою місцевих рекламних оголошень із запасами та інструментів для покупок у прямому ефірі, платформа електронної комерції повинна постійно працювати над тим, щоб залишатися в авангарді технологій.

2.4 Аналіз розвитку електронної комерції в Україні

Дослідження електронної комерції в Україні показало, її розвиток повторює тенденції світового розвитку: у 2020 р. зростання у 41%, тобто на 3,82 млрд. дол., при цьому обсяг експорту склав близько 450 млн. дол.

Структуру експорту електронної комерції наведено на рис. 2.11.

Серед основних Українських трендів є перехід від Інтернет-магазинів до маркетплейсів (маркетплейс – це майданчик, на якому покупець може порівняти й купити товари відразу в кількох продавців. Маркетплейс є своєрідним посередником між споживачем і тим, хто пропонує свої продукти чи послуги. На такому майданчику зазвичай не продаються товари лише одного типу, наприклад, виключно побутова техніка [62].

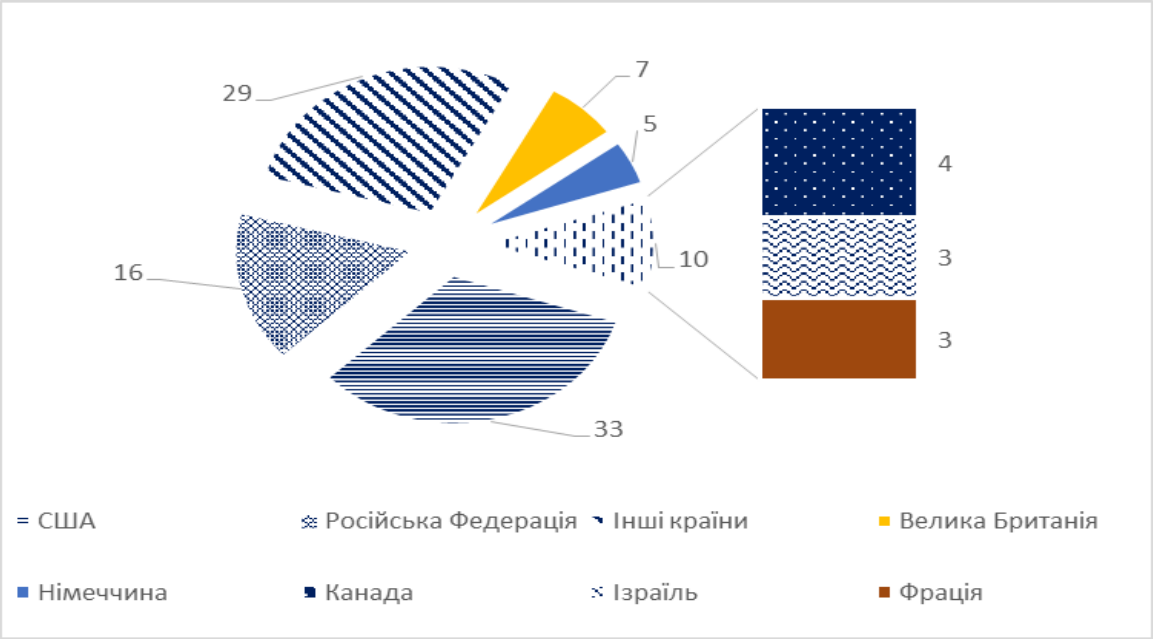

Рисунок 2.11 – Структура експорту електронної комерції

Джерело [62-63]

Продовжується консолідація ринку, розпочата в 2019-2020 роках. У 2019 році найбільше зростання кількості інтернет-магазинів спостерігалося в сегменті великих інтернет-магазинів (+25%), які, незважаючи на невелику кількість (50 організацій), генерують близько 33% загального товарообігу в секторі (рис.2.12).

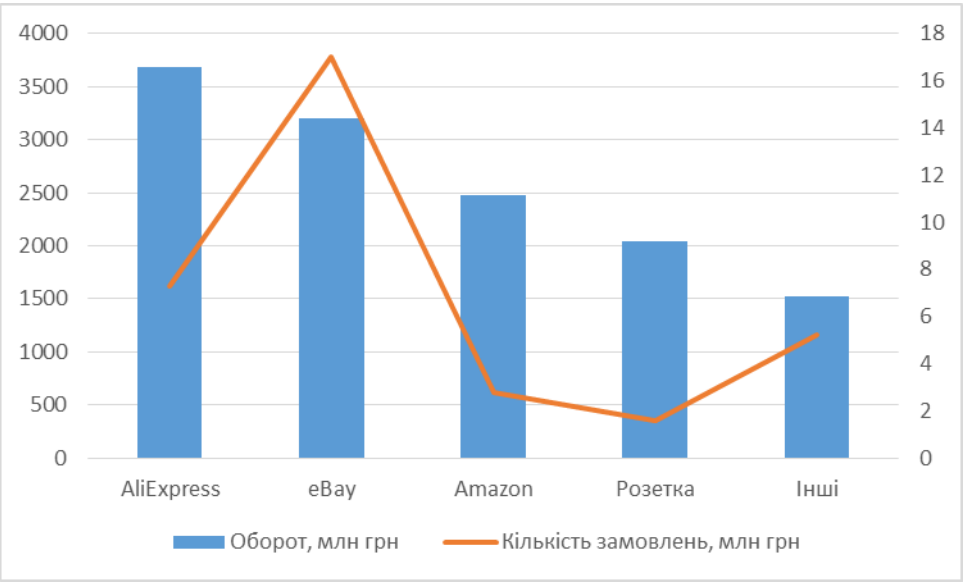

Рисунок 2.12 – Обсяги e-Commerce в Україні

Ще однією тенденцією є зростаюча конкуренція між маркетплейсами та соціальними мережами. В українському Instagram зростає кількість дрібних брендів, і збільшується конкуренція в секторі hand made. Попри це, на сьогодні споживачі в Україні віддають перевагу більшим компаніям в порівнянні з малими. Центр Разумкова слушно відзначає, що у сфері електронної комерції в Україні актуальним залишається тренд монополізації ринків великими суб'єктами бізнесу [64]. Бренди також відповідають на таке стрімке зростання, об'єднуючи разом свої команди з електронної торгівлі та цифрового брендингу, зокрема про такий підхід повідомили 25% маркетологів (рис. 2.13) [65].

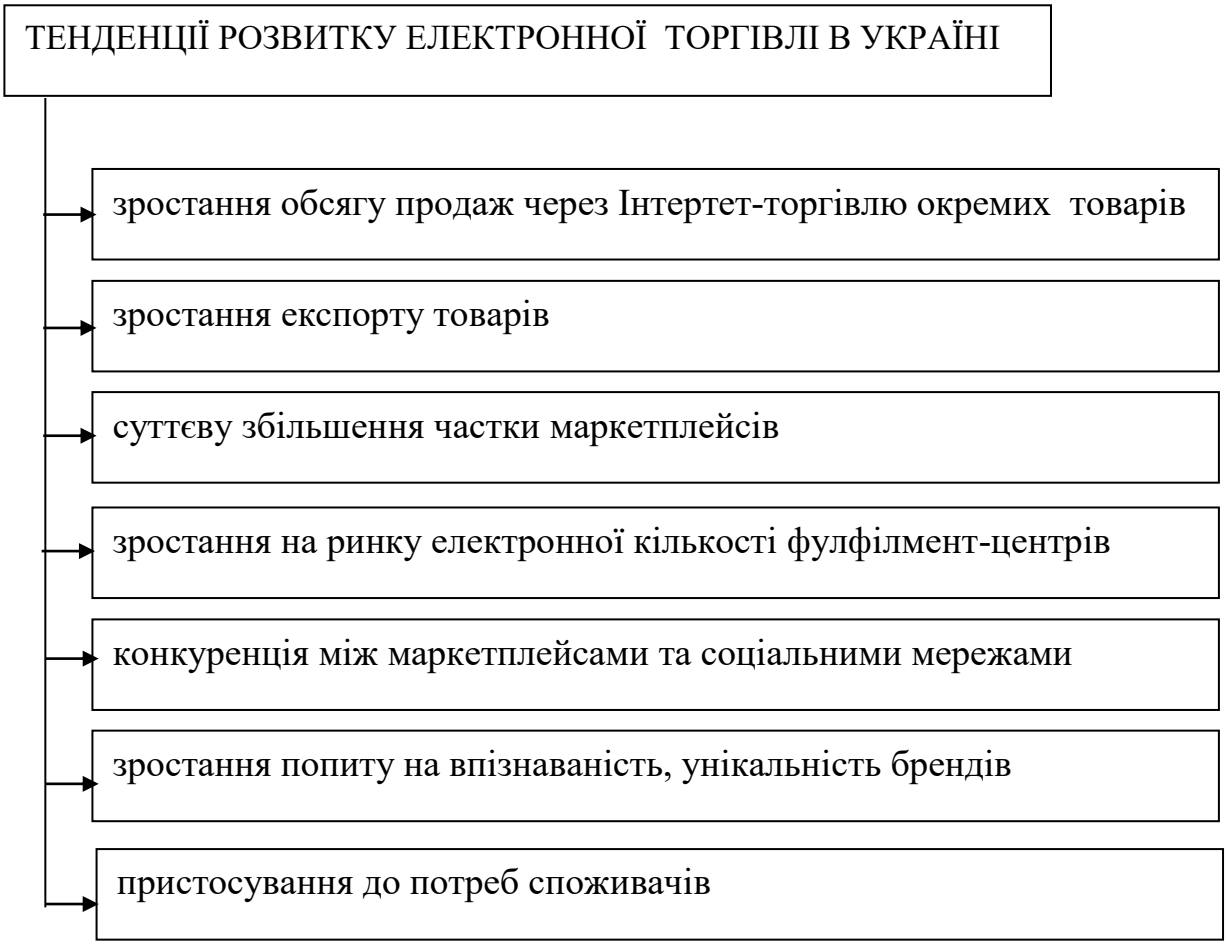

Рисунок 2.13 – Основні тенденції розвитку електронної комерції в Україні

Особливості розвитку електронної комерції в Україні полягають у тому, що, з одного боку, в нашій країні, як не в одній іншій, процеси діджиталізації є дуже активними і динамічними, а, з іншого боку, вітчизняний ринок електронної комерції перебуває на початковій фазі розвитку [66].

Разом з продажами збільшилося навантаження на служби доставки. У головних поштових операторів України «Нова Пошта» та «Укрпошта» кількість посилок збільшилася на 25-35%. Але для клієнтів інтернет-магазинів це не виправдання можливих затримок –вони хочуть швидко отримувати свої замовлення. Ситуація, що склалася, стала поштовхом для розвитку українських служб доставки. За даними Держстату, інвестиції в кур'єрську діяльність за три квартали 2020 року збільшилися в 8 разів - 353,7 млн грн проти 44,7 млн, за аналогічний період минулого року [67].

У результаті виконаних досліджень виявлено, що упродовж останніх років справжніми викликами для суб’єктів електронної комерції стали:

− рівень оподаткування і складність отримати потрібну інформацію;

− недовіра до он-лайн-послуг і їхньої безпечності;

− недоступність електронної-комерції за межами великих міст;

− слабке законодавче врегулювання ринку електронної комерції, що розширює можливості для шахрайства і монополізації ринку.

Щодо можливостей розвитку електронної комерції, то серед них слід виокремити такі: при перенесенні бізнесу в он-лайн, набагато легше аналізувати власну ЦА; формується адаптивне позиціонування суб’єкта підприємництва, яке орієнтоване на споживача; полегшується процедура сплати податків; розширюються можливості формування маркетплейсів; уможливлюється створення простору (платформа/соцмережа) для розвитку малих бізнесів в мережі; завдяки наявності кіберполіції і введення адміністративної та кримінальної відповідальності для шахраїв в сфері

електронної комерції зростання безпечності ведення бізнесу у сфері електронної комерції [68].

Внаслідок прийняття Закону України «Про електронну комерцію» № 675-VIII від 03.09.2015 року, під впливом обставин викликаних пандемією, а також внаслідок загальносвітових тенденцій можна очікувати, що найближчими роками частка ринку е-комерції зростатиме у всіх видах підприємницької діяльності. Інтенсивність цього явища залежатиме від рівня розвитку цифрових комунікацій та інфраструктури ринку.

За дослідженнями фахівців The Future of Ecommerce Report 2021 у попередньому році було кілька яскраво виражених викликів на ринку електронної комерції, а саме: «…бум електронної торгівлі сприяє рекордній он-лайн-конкуренції; нова поведінка споживачів змінює майбутнє роздрібної торгівлі; фулфілмент стає конкурентною відмінністю; побудова бренду утруднена домінуючим становищем маркетплейсів; утримання клієнтів стає головним пріоритетом…».

Висновки до другого розділу

Останні два роки були трансформаційними для індустрії електронної комерції. Він отримав безпрецедентний поштовх через COVID-19 і продовжує зростати сам по собі. Але для того, щоб підтримувати динаміку, підприємствам електронної комерції потрібно зосередитися на створенні змін, не реагуючи на них і швидко переймаючи тенденції, щоб зберегти лояльність існуючих клієнтів і звернутися до нових.

Серйозні зміни в конфіденційність в Інтернеті та те, як її розглядають. Деякі з цих змін потенційно можуть мати великий вплив на електронну комерцію та маркетинг, а деякі вже змінюють ринок. Зростаюча обізнаність

споживачів про проблеми конфіденційності даних створює додаткові проблеми для підприємств електронної комерції. Щоб бізнес електронної комерції випередив конкурентів, він повинен мати унікальну торгову пропозицію.

Сучасні технології відкривають безмежні можливості для бізнесу електронної комерції, проте їх супроводжують і ризики, пов'язані з сучасними технологія ми обробки даних та доступу до особистих даних клієнтів. Від створення цінової стратегії та підвищення гнучкості існуючого рішення для електронної комерції за допомогою безголової електронної комерції до більш ефективного охоплення цільової аудиторії за допомогою місцевих рекламних оголошень із запасами та інструментів для покупок у прямому ефірі, платформа електронної комерції повинна постійно працювати над тим, щоб залишатися в авангарді технологій.

Дослідження електронної комерції в Україні показало, її розвиток повторює тенденції світового розвитку. Серед основних Українських трендів є перехід від Інтернет-магазинів до маркетплейсів. Особливості розвитку електронної комерції в Україні полягають у тому, що, з одного боку, в нашій країні, як не в одній іншій, процеси діджиталізації є дуже активними і динамічними, а, з іншого боку, вітчизняний ринок електронної комерції перебуває на початковій фазі розвитку

3 УДОСКОНАЛЕННЯ УПРАВЛІННЯ БЕЗПЕКОЮ E-COMMERCE ПІДПРИЄМСТВ

3.1 Формування механізму ідентифікації та управління ризиками e-commerce

Метод дослідження поєднує STRIDE та ISSRM методи через процес ітеративної ідентифікації активів, визначення ризиків, обробки ризиків та процедур компромісу між ризиками (рис. 3.1). Результати кожного заходу оцінюються експертами, коли діяльність завершена, щоб визначити, чи є результат кожного кроку задовільним.

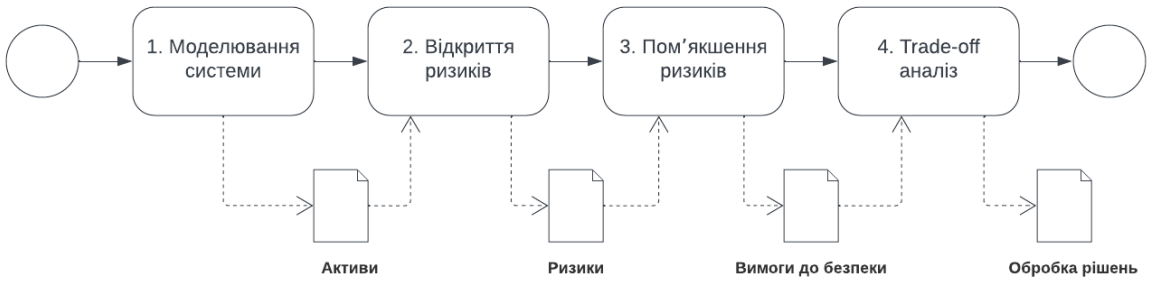

Рисунок 3.1– Застосування підходу, заснованого на загрозах

Модель системи. Ця діяльність визначає системний контекст як перший крок до ідентифікації та визначення сфери застосування процесу управління ризиками. Результатом цієї діяльності є ідентифіковані та проілюстровані активи з використанням відповідного моделювання мови.

Виявлення ризиків. Ця діяльність зосереджена на виявленні ризиків для безпеки платіжного процесу в системі електронної комерції. Він передбачає використання STRIDE для проведення аналізу загроз на ідентифікованих активах в діяльності Модельної системи. Результатом цієї діяльності є ризики, розроблені відповідно до концепцій, пов'язаних з ризиками ISSRM.

Пом'якшення ризиків. Ця діяльність демонструє дії, спрямовані на пом'якшення сценаріїв ризиків визначених в рамках діяльності виявлення ризиків. Результатом цієї діяльності є безпека вимоги щодо захисту системи від виявлених ризиків.

Проаналізувати компроміси. Необхідні зусилля для реагування на ризик, ймовірно, перевищать наявні ресурси. Отже, необхідний аналіз ризиків, пов’язаний з торгівлею. Запроваджено метрику безпеки та процедуру аналізу компромісів для вирішення проблеми управління ресурсами для обробки ризиків безпеки. Для цього використовуються метричні значення активів з діяльності «Моделювання системи», рівні зниження ризиків з діяльності «Виявлення ризиків» для аналізу компромісів збираються дані про вартість реалізації контрзаходів, отримані в результаті діяльності «Пом'якшення ризиків». Результатом цієї діяльності є Ризик-рішення щодо поводження з ризиком.

Система електронної комерції складається з ряду складних процесів та взаємодій, які складно повністю проаналізувати в рамках цієї роботи. Таким чином, ми здійснили цілеспрямований вибір процесу, що лежить в основі систем електронної комерції - процесу виконання замовлень. Процес виконання замовлення на рис. 3.2 складається з ряду процесів, що починаються з процесу «Каталог продукції» для перегляду продукту, процесу «Торговий кошик» для підготовки до перевірки, процесу оплати, що дозволяє придбати вибраний продукт і процесу доставки, який доставляє продукт клієнту, таким чином, завершуючи замовлення.

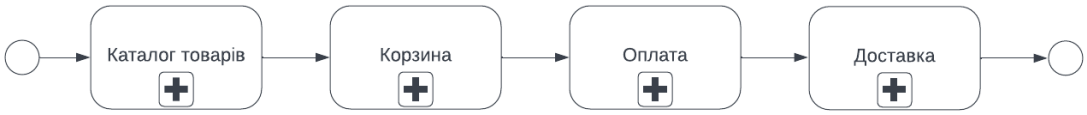

Рисунок 3.2 – Ланцюжок створення вартості процесу виконання замовлення

Процес оплати, зображений на рисунку 3.3, є особливо цікавим процесом у цьому ланцюжку створення вартості, де для завершення транзакцій необхідна конфіденційна інформація про клієнта, продавця та бізнесу. Активи в рамках цього процесу вимагають високого рівня безпеки конфіденційності, цілісності та доступності. Цей процес забезпечує значну кількість атак для аналізу загроз безпеці та управління ризиками, а також досить складне дослідження.

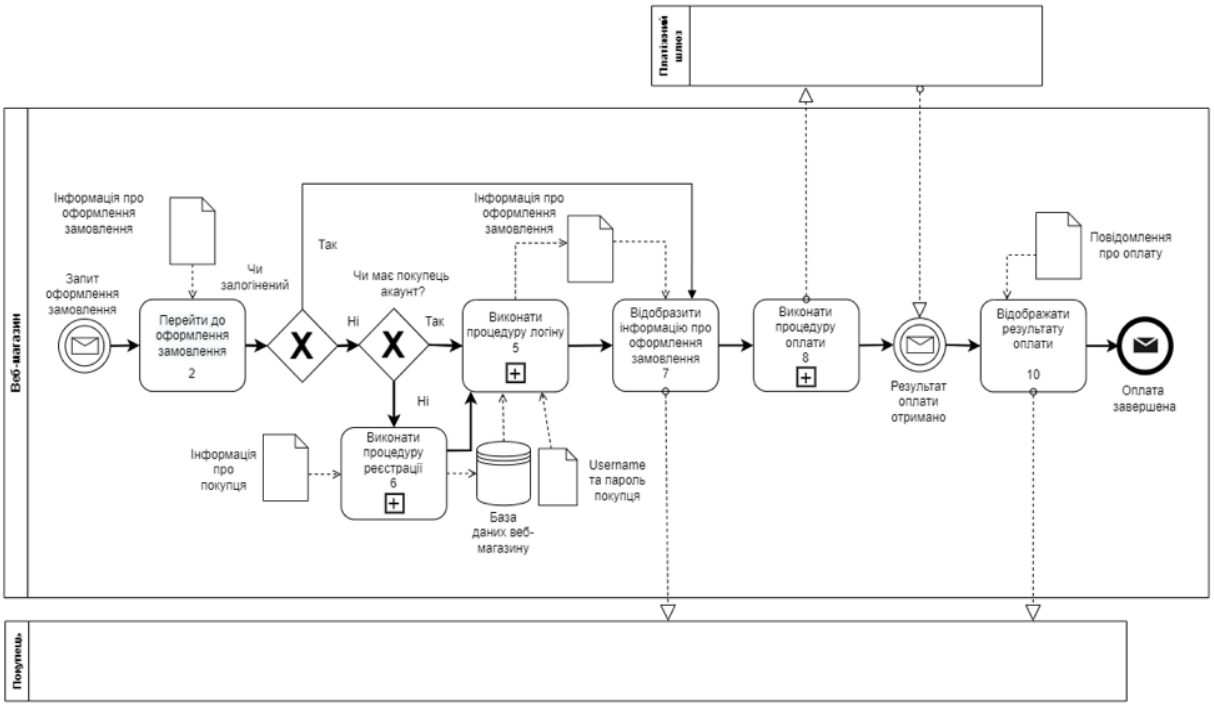

Рисунок 3.3 – Процес оплати в інтернет-магазині електронної комерції

3.2 Практична реалізація запропонованого механізму

Експертна оцінка комбінації STRIDE та ISSRM здійснюється по мірі завершення кожного заходу в рамках підходу, орієнтованого на загрози. Обрані експерти складаються з семи учасників-експертів, цілеспрямовано відібраних на основі їхнього досвіду з розробки та управління програмним

забезпеченням, управління ризиками безпеки та бізнес-процесами. Серед цих експертів були IT-спеціалісти (2) та експерти з досвідом роботи у сфері бізнес-інформаційних технологій (5) (див. таблицю 3.1).

Таблиця 3.1 – Експертна довідка

ID	Позиція	Бекграунд	Досвід роботи в галузі
1	QA Team Lead	10+ років розробки та тестування програмного забезпечення (в тому числі 2 роки досвіду розробки програмного забезпечення, пов'язаного з електронною комерцією)	IT-спеціаліст
2	Team Lead розробки	10+ років досвіду в розробці програмного забезпечення (в тому числі 3 роки досвіду в розробці програмного забезпечення, пов'язаного з електронною комерцією)	IT-спеціаліст
3	Директор кібербезпеки	26+ років в управлінні IT та бізнес IT суміжні ролі	IT-спеціаліст та спеціаліст бізнес IT
4	Team Lead для Оперативного центру з питань безпеки	20+ років досвіду в управлінні IT та ролях, пов'язаних з IT в бізнесі	IT-спеціаліст та спеціаліст бізнес IT
5	Інженер кібербезпеки	7+ років досвіду, включаючи бізнес IT розробка програмного забезпечення, пов'язаного з управлінням та електронною комерцією	IT-спеціаліст та спеціаліст бізнес IT
6	Інженер кібербезпеки	7+ років досвіду, включаючи бізнес IT та управління IT-інфраструктурою	IT-спеціаліст та спеціаліст бізнес IT
7	Технічний спеціаліст з продукції	4+ роки досвіду роботи в IT, включаючи бізнес дослідження управління бізнес-процесами	IT-спеціаліст та спеціаліст бізнес IT

Експерти запрошувалися до цільової дискусії для оцінки процесу та результатів. Оцінка базується на коректності ілюстрацій моделі, актуальності дослідницького методу діяльності та користі від поєднання STRIDE та ISSRM. Наприкінці кожної ітерації оцінювання кожного виду діяльності були визнані задовільними.

Далі описані результати аналізу, що демонструють життєздатність поєднання STRIDE та ISSRM у платіжному процесі інтернет-магазину електронної комерції для виявлення та мінімізації загроз.

Процес оплати, показаний на рисунку 3.3, підтримується низкою системних активів та процесів. Ця підтримка включає додаток електронної комерції Інтернет-магазин. Цей додаток складається з сервера, який обробляє запити, тобто запити на вхід або оформлення замовлення. Для входу в систему запитів, Інтернет-магазин використовує свій процес входу в систему (див. рисунок 3.4), де ім'я користувача та пароль як бізнес-актив надається Інтернет-магазину (системний актив) через його інтерфейс входу (системний актив) для аутентифікації та авторизації клієнта перед продовженням процесу оплати.

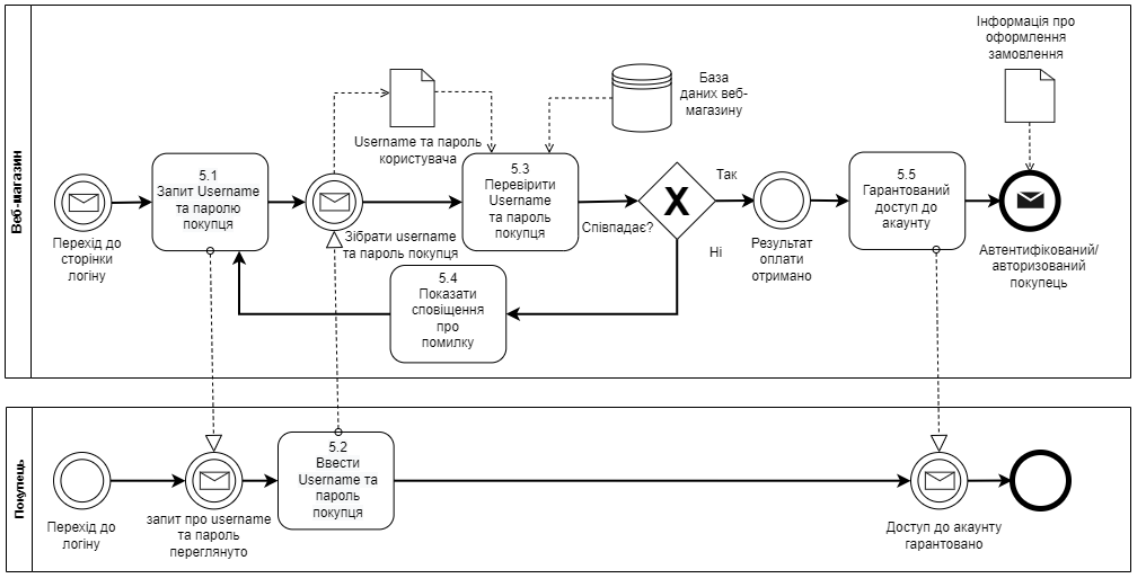

Рисунок 3.4 – Процес входу в інтернет-магазин для здійснення електронної комерції

Відповідно до наведеного вище опису, бізнес-активи та система їх підтримки для дослідження виокремлено з його бізнес-процесу та описано в таблиці 3.2. Після завершення цієї роботи експерти оцінили коректність BPMN-моделей, що використовуються для представлення активів, та якість виявлених активів. Експерти визнали BPMN відповідною мовою моделювання для виявлення активів для платіжного процесу. Кінцевими результатами цієї діяльності є бізнес та системні активи які показано в таблиці 3.2.

Таблиця 3.2 – Активи в розрахунках

Системні активи	Підтримувані бізнес-активи
Інтерфейс входу в інтернет-магазин, клієнт, база даних інтернет-магазину	Процедура здійснення входу в систему, Логін і пароль, Інформація про клієнта
Сервер інтернет-магазину, інтернет-магазин, клієнт	Сервіс оформлення замовлення в інтернет-магазині, Інформація про замовлення
Сервер веб-магазину, клієнт	Ідентифікатор сесії клієнта
База даних веб-магазину, сервер веб-магазину	Логи сервера веб-магазину

Для аналізу ризиків безпеки використовується процес здійснення авторизації в рамках платіжного процесу. Загрози безпеці виникають внаслідок існування агентів загроз та вразливостей в активах системи. Для аналізу було обрано деякі системні активи. До них відносяться інтерфейс входу до веб-магазину, сервер веб-магазину та веб-магазин для демонстрації підходу, що ґрунтується на оцінці загроз. Ми використали базу даних вразливостей CWE для виявлення потенційних вразливостей розглянутих системних активів (див. таблицю 3.3).

Таблиця 3.3 – Вразливості ідентифікованих системних активів

Системний актив	Потенційні вразливості	CWE2020
Інтерфейс входу в інтернет-магазин	Відсутність валідації вхідних даних в інтерфейсі входу в інтернет-магазин	CWE-20
Сервер інтернет-магазину	Неправильна нейтралізація виводу для логів сервера інтернет-магазину, неправильна логіка перевірки замовлень на сервері інтернет-магазину, виділення ресурсів без лімітів і дроселювання в сервері інтернет-магазину	CWE-117 CWE-285 CWE-770
Інтернет-магазин	Слабка парольна аутентифікація	CWE-521

Для того, щоб обмежити наш аналіз ризиків не аналізуються всі можливі загрози для системи електронної комерції, а виділяється одна загроза за категорією STRIDE електронної комерції, для вразливих активів системи, що наведені в таблиці 3.4. Тут ST - загроза підробки, TT - загроза втручання, RT - загроза відмови, IT - загроза розкриття інформації, DT - загроза відмови в обслуговуванні, ET - загроза підвищення привілеїв.

Кожна розроблена загроза STRIDE та відповідна їй вразливість (V) з таблиці 3.3 відповідає концепціям, пов'язаним з ризиками ISSRM, для визначення впливу загрози у разі успішної експлуатації вразливості (див. таблицю 3.4 - колонка 2). На основі цього аналізу впливу, ми розробляємо сценарій ризиків для безпеки.

Таблиця 3.4 - колонка 3 ілюструє ризики безпеки, де SR - ризик підробки, TR - ризик фальсифікації, RR - ризик відмови, IR - ризик розкриття інформації, DR - ризик відмови в обслуговуванні та ER - ризик підвищення привілеїв.

Таблиця 3.4 – Аналіз впливу на ризики виявлених загроз програми STRIDE та її вимоги до безпеки

Тип загрози	Аналіз впливу	Ризик безпеки	Вимоги до безпеки
S	ST1: Зловмисник отримує доступ до дійсної сесії клієнта. V: Слабка генерація ідентифікатора сеансу на сервері інтернет-магазину. Наслідки: Втрата конфіденційності ідентифікатора сеансу клієнта.	SR1: Зловмисник порівнює дійсні ідентифікатори сеансів і намагається отримати доступ до дійсного сеансу клієнта, використовуючи слабкий ідентифікатор сеансу, згенерований сервером Інтернет-магазину, що призводить до втрати конфіденційності id сеансу клієнта.	SR1.SReq1: Алгоритм генерації ідентифікатора сесії серверу інтернет-магазину повинен бути стійким до перебору. SR1.SReq2: Інтернет-магазин не повинен допускати дублікатів одночасних сесій користувачів, що походять з різних машин.
T	TT1: Зловмисник модифікує JavaScript код веб-магазину, щоб модифікувати інформацію про замовлення на сайті, використовуючи неправильну логіку перевірки замовлень сервера Інтернет-магазину. V: Неправильна перевірка замовлень Логіка роботи сервера веб-магазину. Наслідки: Втрата цілісності Інформації про оформлення замовлення.	TR1: Зловмисник модифікує JavaScript код веб-магазину для зміни інформації про замовлення на касі, використовуючи Неправильну перевірку замовлення. Логіку роботи сервера Інтернет-магазину, що призводить до втрати Цілісності оформлення замовлення Інформації.	TR1.SReq1: Інтернет-магазин повинен відхиляти зміни до інформації про замовлення після того, як Клієнт перейшов до оформлення замовлення. TR2.SReq2: Інтернет-магазин повинен запобігати несанкціонованому спотворення інформації про замовлення інформації про замовлення під час процесу оплати.

Продовження таблиці 3.4

R	RT1: Зловмисник додає записи в логи сервера Webshop, щоб замаскувати незаконні транзакції в Webshop. V: Неправильна нейтралізація виводу для логів сервера інтернет-магазину. Наслідки: Втрата цілісності логів сервера веб-магазину.	RR1: Зловмисник додає записи в логи сервера веб-магазину для маскування незаконних транзакцій у веб-магазині, використовуючи неправильну нейтралізацію виводу до логів сервера, що призводить до порушення цілісності логів сервера Інтернет-магазину.	RR1.SReq1: Інтернет-магазин повинен перевірити, що логи реєстрації захищені від несанкціонованого доступу та модифікації. RR1.SReq2: Інтернет-магазин повинен перевірити, що виведення логу належним чином нейтралізується в записах логу.
I	IT1: Зловмисник витягує конфіденційну інформацію про клієнтів зі сховища веб-магазину шляхом відправки підроблених SQL запитів через інтерфейс інтернет-магазину входу в базу даних. V: Відсутність перевірки вхідних даних в інтерфейсі входу до веб-магазину. Наслідки: Втрата конфіденційності інформації про клієнтів.	IR1: Зловмисник витягує Інформацію про клієнта зі сховища інтернет-магазину, відправляючи підроблені SQL ін'єкції через інтерфейс входу в інтернет-магазин через інтерфейс входу в систему, використовуючи відсутність валідації вхідних даних інтерфейсу входу в інтернет-магазин, що призводить до втрати конфіденційності інформації Клієнта.	IR1.SReq1: Інтернет-магазин повинен перевірити, що вхідні дані канонізовані перед валідацією. IR1.SReq2: Інтерфейс входу в систему повинен повторно перевіряти вхідні дані в параметризованих збережених процедур. IR1.SReq3: Інтернет-магазин повинен перевірити, що він не виводить повідомлення про помилки що містять конфіденційні

Продовження таблиці 3.4

			дані. IR1.SReq4: Інтернет-магазин повинен використовувати тільки параметризовані збережені процедури для запитів до бази даних інтернет-магазину.
D	DT1: Зловмисник виснажує сервіс оформлення замовлення в інтернет-магазині за допомогою численних запитів на оформлення замовлення. V: Розподіл ресурсів без обмежень або дроселювання на сервері інтернет-магазину. Наслідки: Втрата доступності Сервісу оформлення замовлення в інтернет-магазині.	DR1: Зловмисник завалює сервер безліччю запитів на оформлення замовлення і виснажує сервіс оформлення замовлення інтернет-магазину, експлуатуючи виділені сервером ресурсів без обмежень або Дроселювання, що призводить до втрати доступності інтернет-магазину оформлення замовлення.	DR1.SReq1: Компоненти веб-магазину повинні мати налаштовані обмеження масштабу. DR1.SReq2: Інтернет-магазин повинен мати прийнятну поведінку, визначену для випадків, коли розподіл ресурсів досягає граничних значень.
E	ET1: Зловмисник використовує слабку аутентифікацію на основі пароля, налаштовану в інтернет-магазині, щоб отримати повні привілеї до інформації користувача. V: Слабка аутентифікація на основі пароля,	ER1: Зловмисник використовує слабку аутентифікацію на основі пароля, налаштовану в інтернет-магазині, щоб отримати повні привілеї до інформації про клієнта, що призводить до	ER1.SReq1: Інтернет-магазин повинен мати налаштовану політику надійних паролів. ER1.SReq2: Інтернет-магазин повинен обмежити кількість виявлених спроб доступу, які не

Продовження таблиці 3.4

	налаштована у веб-магазині. Наслідки: Втрата конфіденційності та цілісності інформації про клієнта.	втрати конфіденційності та цілісності інформації про клієнта.	відповідають вимогам автентифікації, до 5 спроб.

Цей аналіз ризиків відповідає моделі домену ISSRM (див. рисунок 3.1), де загроза безпеці викликає подію безпеки (конкретизовану в аналізі впливу), а подія безпеки викликає 0...1 ризик безпеки, що призводить до співвідношення один до одного між загрозами в колонці «Аналіз впливу» та ризиками безпеки в колонці «Ризик безпеки» у таблиці 3.4.

Експерти оцінювали цю діяльність, виходячи з якості сценаріїв ризиків та дотримання моделі ISSRM при розробці сценаріїв ризиків. Це призвело до ітеративного оновлення сценаріїв відмови від привілеїв та підвищення рівня ризику безпеки привілеїв. Очевидні переваги використання системи STRIDE для аналізу загроз з метою підтримки ідентифікації ризиків, включаючи продемонстровану простежуваність STRIDE, яка пов'язує ідентифіковані загрози безпеці з ризиками ідентифіковані загрози безпеці з ризиками для безпеки.

Для обробки виявлених ризиків були визначені вимоги безпеки (SReq), наведені в таблиці 3.4 для кожного сценарію ризику, щоб захистити систему від кожного ризику. Ці вимоги позначені відповідно до їх структури ризиків безпеки з додаванням вимог ідентифікатору безпеки (SReq). На рисунку 3.5 показано застосування вимог безпеки до процесу здійснення входу в систему, а на рисунку 3.6 - узагальнене застосування всіх вимог безпеки до процесу здійснення платежів в електронній комерції. Застосування вимог безпеки до бізнес-процесу також призвело до впровадження контрзаходів у системі (див. рис. 3.5). Такі контрзаходи включають механізми перевірки вхідних даних, блокування рахунку клієнта, припинення інших сесій клієнта. Вимоги до безпеки, визначені для зменшення ризиків безпеки, були оцінені відповідно

до характеристик якості, яким повинна відповідати хороша специфікація вимог [69,70]. Окрему увагу було приділено BPMN-ілюстрації вимог безпеки до бізнес-процесу, враховуючи не тільки її синтаксичну правильність, але й здатність ілюструвати обмеження вимог до конкретних активів.

Застосовуємо рішення щодо зниження ризиків для безпеки. Для цього рішення здійснюється управління ресурсами у вигляді аналізу компромісів з метою зниження ризику (див. табл.3.5). Компромісний аналіз використовує метричні значення бізнес-активів (BV), критерій безпеки (SC) для бізнес-активів, потенційні рівні зниження ризику (RRL) та вартість контрзаходів (CC). Ми представляємо метричні значення для бізнес-активів та критерій безпеки цих активів за шкалою від 1 до 3. Рівні зниження ризиків оцінюються за результатами розрахунків ймовірності настання ризикових подій, впливу ризиків та метрик рівня ризиків [71].

Ризикова подія = ймовірність загрози + рівень вразливості – 1.

Вплив = максимальне значення критерію безпеки.

Рівень ризику = ризикова подія * вплив.

Рівень зниження ризику = рівень ризику 1 - рівень ризику 2.

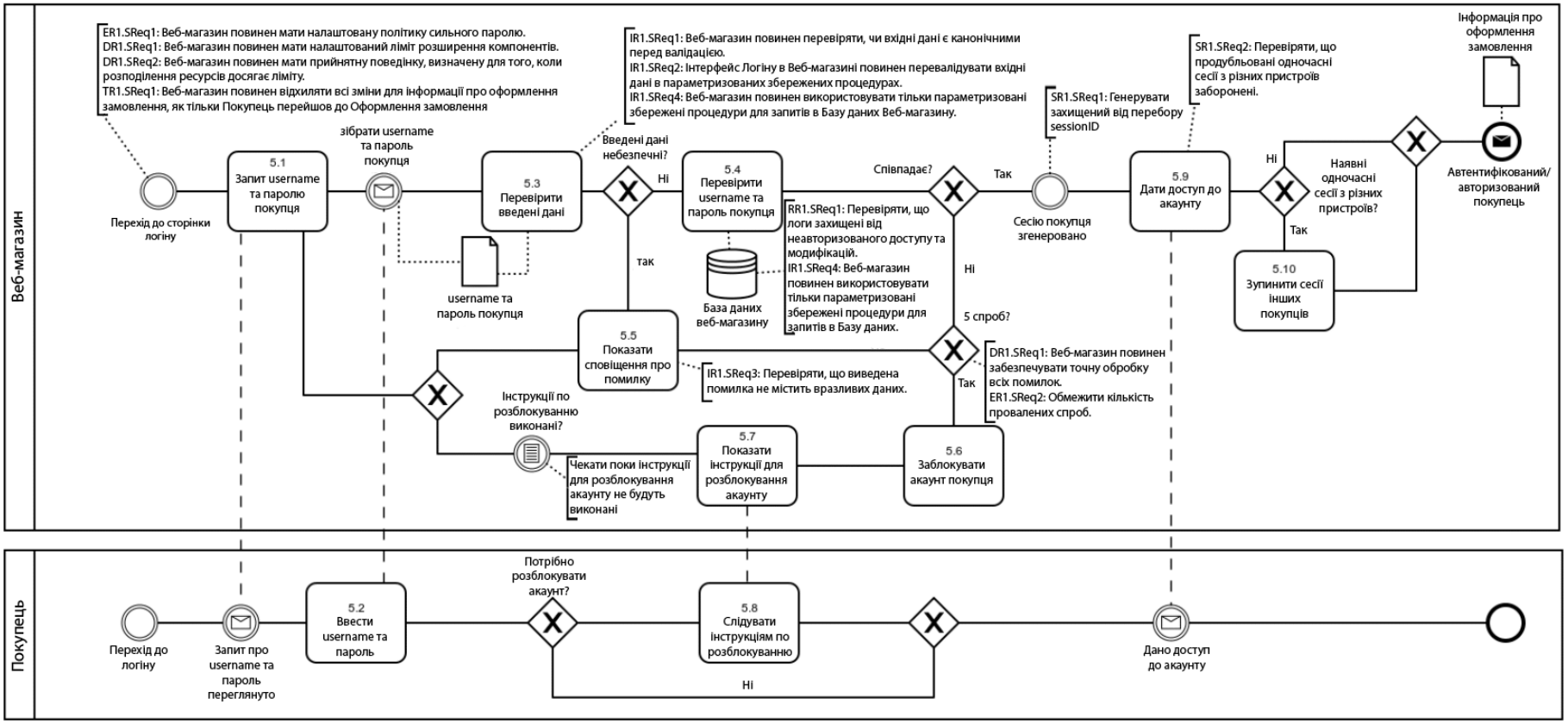

Рисунок 3.5 – Реалізація контрзаходів щодо здійснення процесу входу в систему

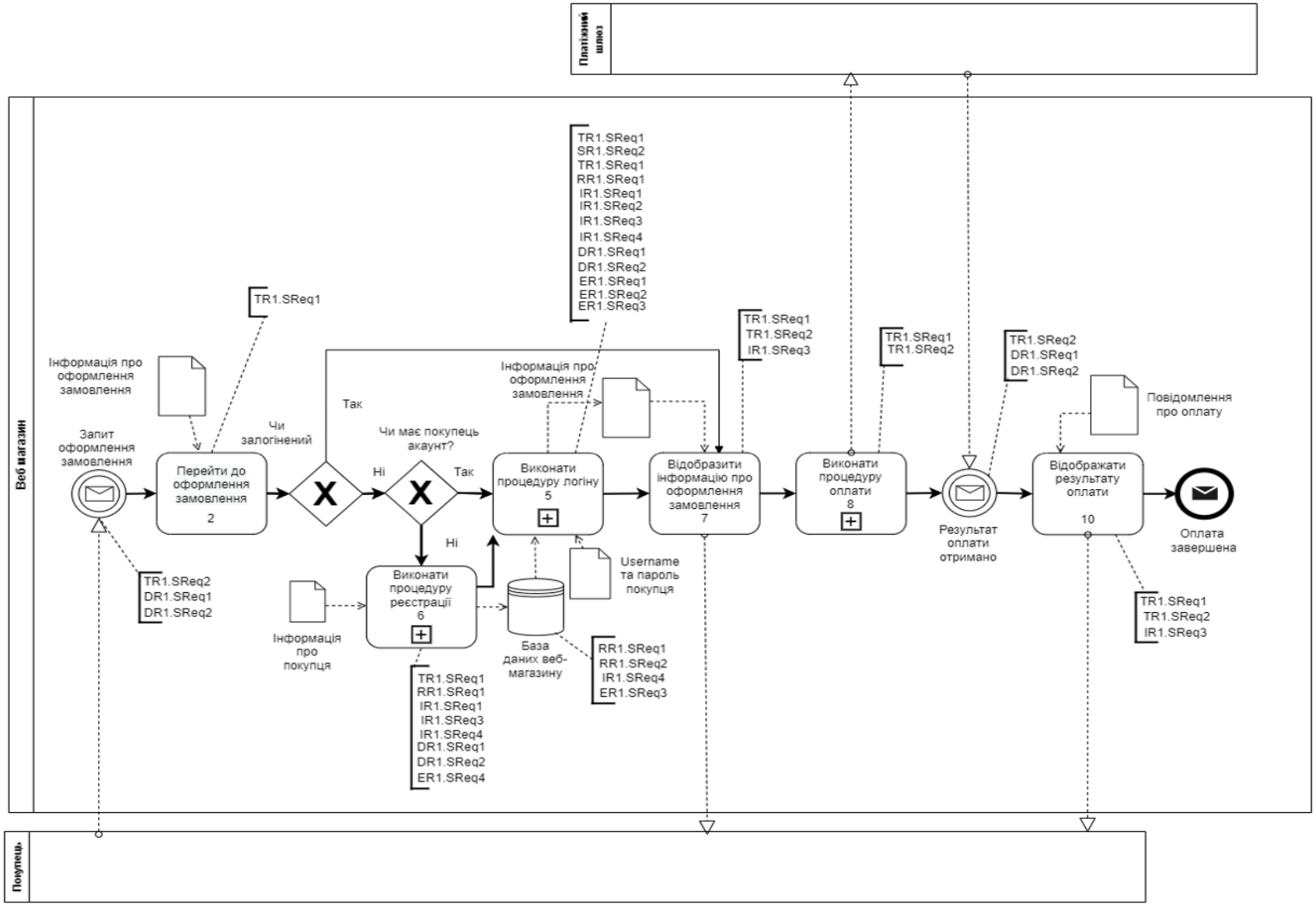

Рисунок 3.6 – Діаграма протидії платіжному процесу

Значення рівня вразливості (VL) та ймовірності загрози (TL) визначалися на основі інформації [72-73] щодо цих сценаріїв. Оцінки витрат на реалізацію контрзаходів були зроблені на основі обґрунтованих рішень, заснованих на запропонованих засобах контролю та вимогах до безпеки щодо сценаріїв ризику.

Рівень загрози (TL1) та рівні вразливості (VL1) для кожного сценарію ризику до обробки ризиків. Оцінки також зроблені для рівня загрози (TL2) та рівня вразливості (VL2) після обробки ризиків. Потім ми отримали оцінки впливу ризиків та потенційного рівня зниження ризику (RRL).

Таблиця 3.5 – Метрики ризиків до та після лікування ризиків

	BV	SC	TL1	VL1	TL2	VL2	RRL	CC
SR1	3	3	2	3	1	1	9	2
TR1	3	3	3	3	2	1	9	3
RR1	2	3	2	2	1	1	6	3
IR1	3	3	3	3	1	1	12	2
DR1	3	3	3	3	1	1	12	2
ER1	3	3	3	3	2	1	9	2

Далі ми розміщуємо ризики, на які необхідно реагувати, у квадрантах графіка, пропонуючи три можливі варіанти позначені як високий - 3 (оптимальне реагування на ризики), середній - 2 (більш складне реагування на менші ризики) та низький - 1 (витратне реагування на менші ризики) на основі отриманих метрик.

Рівень зниження ризиків (RRL) у порівнянні з вартістю бізнес-активів (BV). Бажаною є ситуація, коли актив з високою вартістю бізнесу має високе значення рівня зниження ризику (IR1 та DR1), що має високий пріоритет.

Ризики середньої пріоритетності характеризуються високою вартістю бізнес-активів та низьким рівнем зниження ризиків, а також високим рівнем зниження ризиків та низькою вартістю бізнес-активів (SR1, TR1 та ER1). Найменш бажаною ситуацією є ризик з низькою вартістю бізнес-активів та низьким рівнем зниження ризику (RR1). Це проілюстровано на рисунку 3.7.

Рівень зниження ризику (RRL) та вартість контрзаходів (CC). Бажана ситуація це ситуація з низькою вартістю контрзаходів та високим значенням зниження ризику (RR1), що відповідає високому пріоритету.

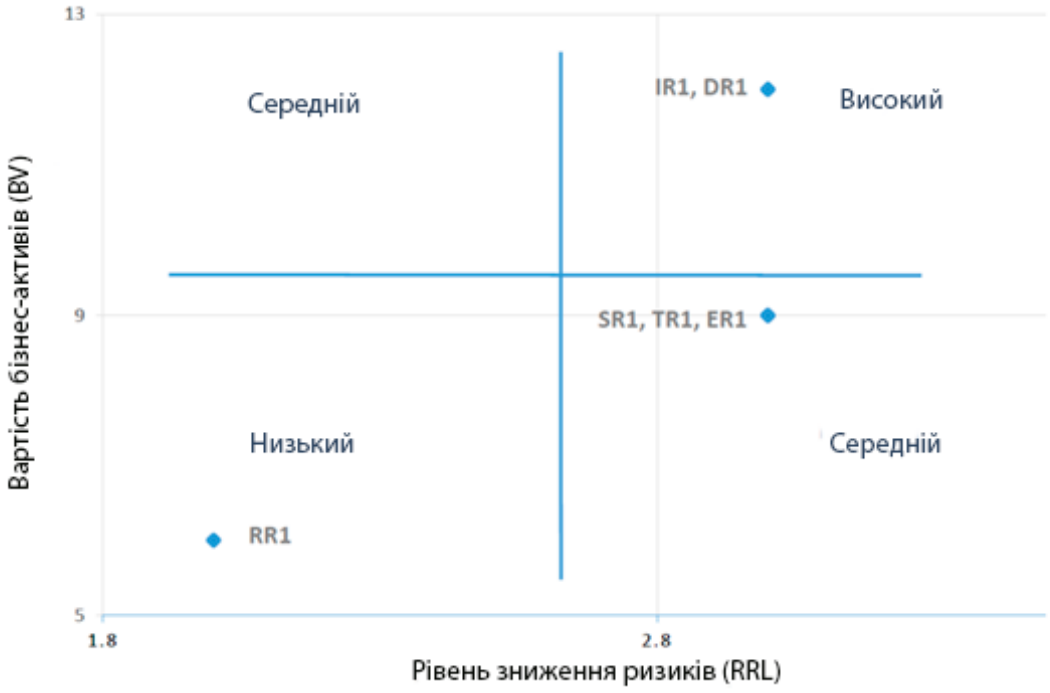

Рисунок 3.7 – Рівень зниження ризиків (RRL) та вартість активів бізнесу (BV)

Середній пріоритет мають квадранти з високою вартістю значення контрзаходів з високим рівнем зниження ризику (TR1) та низькою вартістю контрзаходів з низьким значенням зниження ризику. Низько пріоритетні ризики знаходяться у квадранті з високою вартістю контрзаходів та низьким

значенням рівня зниження ризику (SR1, IR1, DR1 та ER1). Це проілюстровано на рисунку 3.8.

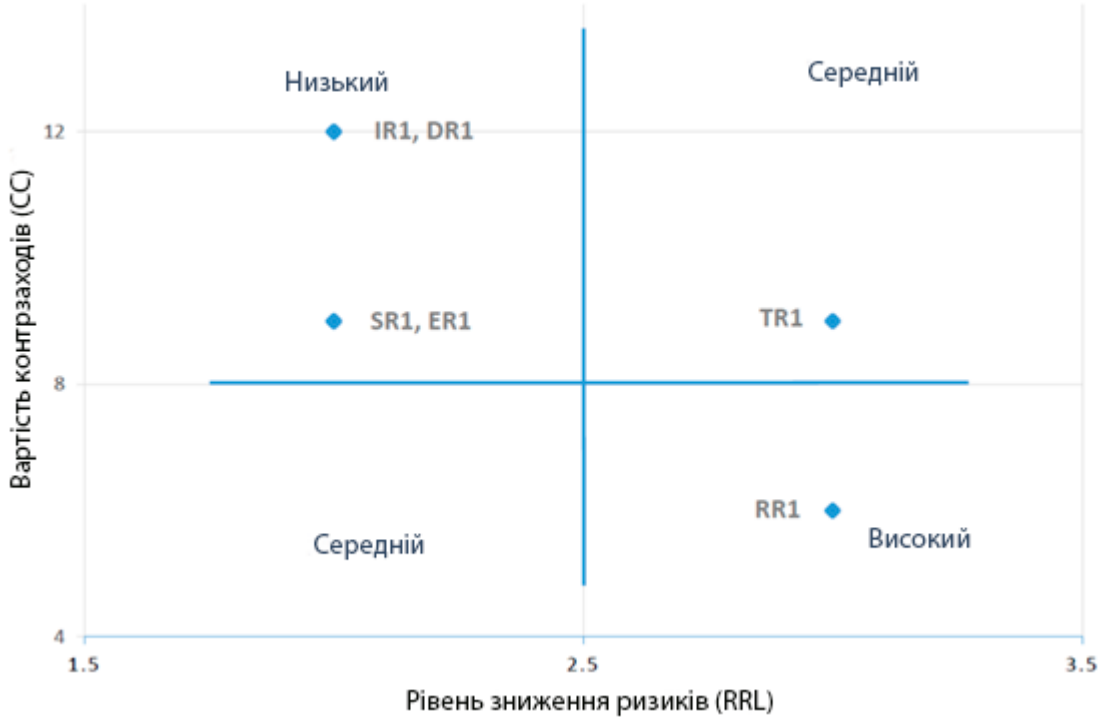

Рисунок 3.8 – Рівень зниження ризиків (RRL) та вартість контрзаходів (CC)

Вартість контрзаходів (CC) у порівнянні з вартістю бізнес-активів (BV). Ризики з високим пріоритетом знаходяться у квадранті з низькою вартістю контрзаходів та високою вартістю бізнес-активів (SR1, IR1, IR2, IR3, IR4, IR5). Середній пріоритет мають квадранти, що мають бізнес-активи високої вартості з високою вартістю контрзаходів (TR1) та комбінація бізнес-активів низької вартості з низькою вартістю контрзаходів. Найменш бажаною ситуація - це ситуація з низькою вартістю бізнес-активів та високою вартістю контрзаходів (RR1). Це проілюстровано на рисунку 3.9.

Таким чином, на основі графіків (рис. 3.7-3.9), які показують ризики, що можуть розглядатися як високо пріоритетні за умови оптимального

реагування. Отримані показники та аналіз компромісів були оцінені експертами та визнані задовільними (табл.3.6).

Рисунок 3.9 – Вартість контрзаходів (CC) та вартість бізнес-активів (BV)

Таблиця 3.6 – Результати аналізу компромісів між ризиками для безпеки

ID ризику	RRLvs BV	RRL vs CC	CC vs BV		Пріоритет
IR1	3	1	3	7	Високий пріоритет
DR1	3	1	3	7	Високий пріоритет
SR1	2	1	3	6	Середній пріоритет
TR1	2	2	2	6	Середній пріоритет
ER1	2	1	3	6	Середній пріоритет
RR1	1	3	1	5	Низький пріоритет

3.3 Аналіз запропонованого підходу до управління ризиками

Запропонований для використання метод STRIDE для підтримки зусиль ISSRM, спрямовані на формування підходу, орієнтованого на боротьбу із загрозами і таким чином забезпечення безпеки. Далі розглянемо, наскільки добре комбінація STRIDE і ISSRM задовольняє наведені причини для поєднання.

Моделювання загроз. Конструкти STRIDE стали основою для ідентифікації загроз як показано в таблиці 3.4. Загрози, що виникають в результаті застосування кожної з конструкцій STRIDE, були легко ідентифіковані та визначені для зазначених системних активів. Ця методика моделювання загроз відповідає доменній моделі ISSRM, що дозволяє конкретизувати концепції, пов'язані з ризиками. Вразливості активів були доповнені з використанням каталогів/бази даних (наприклад, Національної бази даних вразливостей, Переліку загальних слабких місць, а також методів і впливів агентів загроз. Процес моделювання загроз в рамках діяльності «Виявлення ризиків» здійснювався ітеративно з урахуванням експертних оцінок та аналізу для створення таблиці ризиків (див. табл. 3.4).

Категоризація загроз. Загрози безпеці були визначені та класифіковані відповідно до категорій STRIDE. Однак, при класифікації були деякі міркування. При аналізі загроз в якості об’єктів загроз виступають активи. Для загрози спуфінгу (див. табл. 3.4) зловмисник порівнює дійсні ідентифікатори сесії, надані Інтернет-магазином, і методом перебору отримує доступ до дійсної сесії клієнта, при цьому зловмисник використовує інформацію, що розкривається Інтернет-магазином шляхом спостереження за виданими ідентифікаторами сесії, для генерування дійсних ідентифікаторів сесії. Хоча існує певне розкриття інформації, що призводить до можливості здійснення атаки підміни, система не зазнає атаки, якщо розкрита інформація

не використовується для підміни або інших цілей. Розкрита інформація є лише вразливістю на даний момент, а не загрозою.

Інша перспектива, що розглядається, полягає в тому, що відбувається після того, як зловмисник отримує доступ до сеансу клієнта і тепер має більш високі привілеї ніж клієнт. Це можна класифікувати як загрозу підвищення привілеїв (E). Однак, для цього дослідження загрози на даному етапі класифікуються на основі першого впливу. Таким чином, ця загроза в кінцевому підсумку була класифікована як загроза підміни (S).

Вираження вимог безпеки. Вимоги безпеки, виражені в рамках Структури STRIDE допомогли у визначенні та формулюванні вимог безпеки. Хоча вони не надають повного переліку вимог безпеки для конкретного сценарію ризику, вони служать чудовою відправною точкою для визначення вимог безпеки. Кожна отримана вимога безпеки представлена в бізнес-процесі. Ця ілюстрація показує зацікавленим сторонам та системним архітекторам, де вимоги безпеки можуть бути застосовані, а засоби контролю безпеки впроваджені з метою забезпечення безпеки.

Простежуваність. В рамках процесу аналізу та оцінки ризиків ISSRM (включаючи ідентифікацію загроз до класифікації), було виявлено простежуваність з використанням STRIDE. Було виявлено, що недостатньо просто перерахувати виявлені ризики безпеці, але необхідно забезпечити простежуваність до пов'язаної з ним загрози. Наприклад, всі ризики в результаті загрози спуфінгу позначаються як SRx, де x - номер ризику. Тепер в рамках наступного процесу обробки ризиків та визначення (і формулювання) вимог безпеки, розроблені вимоги безпеки були зроблені таким чином, щоб їх можна було простежити до ризику безпеки і, таким чином, до класифікації загроз, яка породила вимогу. Наприклад, вимогам безпеки, що генеруються в результаті ризику підміни, присвоюється мітка SRx.SReqx', де x - номер ризику, а x' - номер вимоги безпеки.

Контрзахідна пропозиція. Пропозиція щодо контрзаходів є похідною від вимог безпеки для сценаріїв ризику для безпеки. На рисунку 3.9 видно, що застосування вимог безпеки до процесу здійснення входу в систему призвело до реалізації контрзаходів безпеки, таких як блокування доступу до облікового запису після 5 спроб, перевірка вводу на валідність даних користувача та перевірка наявності паралельних перевірка наявності паралельних клієнтських сесій.

Вираження потреб у безпеці. Потреби в безпеці системи електронної комерції оцінюються під час сценарію аналізу ризиків безпеки (див. табл. 3.6) та з урахуванням ризику підміни, який є ризиком, пов'язаним з аутентифікацією для системи електронної комерції, ризиком несанкціонованого втручання ризик підробки, пов'язаний з цілісністю, а також решта сценаріїв ризиків безпеки відповідно до властивостей безпеки STRIDE. Це допомогло виявити та визначити потреби в безпеці бізнес-активів в рамках цього сценарію.

Відповідні підходи, розглянуті раніше показали дослідження аналізу захищеності інформаційних систем з використанням STRIDE, комбінації STRIDE з іншими методами аналізу безпеки та комбінації методу аналізу загроз безпеці - Security-Risk Oriented Patterns (SRP) та ISSRM. Використання одного методу аналізу загроз безпеки або комбінації методів аналізу загроз методів [50,17,23] не дозволяло ефективно управляти отриманими ризиками безпеки. Комбінація STRIDE та ISSRM використовує STRIDE для аналізу загроз безпеці, а ISSRM - для управління ризиками, що виникають в результаті аналізу загроз, проведеного STRIDE. Це управління включає в себе визначення вимог безпеки для захисту системи від проаналізованих загроз пропозицію контрзаходів та аналіз компромісів для управління ресурсами при обробці ризиків.

Існують також дослідження, в яких метод аналізу загроз безпеці поєднується з методом управління ризиками безпеки. Тут метод ISSRM був

поєднаний з моделями, орієнтованими на ризики безпеки, для забезпечення безпеки процесу відновлення діяльності авіакомпанії процесу. Хоча ризик-орієнтовані моделі безпеки є хорошим інструментом для аналізу загроз безпеці, вони мають обмеження. SRP обмежені рамками системного бізнес-процесу. З іншого боку, STRIDE аналіз загроз безпеці в системі не обмежується представленням бізнес-процесів. STRIDE відкрита для інших представлень, таких як діаграми потоків даних (DFD), не обмежених бізнес-процесом. У цій роботі, використання методів бізнес-моделювання (тобто BPMN) використовується для розгляду активів, ризиків і сценаріїв обробки ризиків, Однак аналіз не обмежувався лише активами, проілюстрованими в моделях. SRP містить 5 моделей для аналізу загроз безпеки, і ці моделі не охоплюють стільки ж потреб у безпеці системи, як у STRIDE. STRIDE не використовує патерни, але містить властивості безпеки, що виражають (у своїх протилежностях) потреби в безпеці системи. Сценарії використовуються для забезпечення розширеної комунікації щодо ризиків безпеки між IT та бізнес зацікавленими сторонами, які беруть участь у ризиках безпеки. За результатами обговорення, поєднання STRIDE та ISSRM надало перевагу у порівнянні з окремим використанням STRIDE та комбінаціями між іншими методами аналізу загроз безпеці. Те ж саме можна сказати і про інші комбінації методів аналізу загроз безпеці з ISSRM. Цей підхід використовував переваги STRIDE та ISSRM, надаючи експертну оцінку аналізу системних загроз, ризиків, зменшення ризиків та аналізу компромісів для управління ризиками безпеки.

Висновки до третього розділу

Аналіз впливу комбінації STRIDE та ISSRM на платіжний процес, об'єднані разом у наданні відповіді на питання: Як ми можемо підтримати управління ризиками безпеки за допомогою цільового підходу до аналізу загроз безпеці? Запропоновано підхід, орієнтований на загрози, що оцінюються експертами з безпеки, для управління ризиками безпеки запропоновано та проаналізовано підхід, заснований на оцінці загроз експертами з безпеки для управління ризиками безпеки. При цьому аналізується використання методу аналізу загроз безпеці - STRIDE для демонстрації інтенсивного аналізу загроз безпеці, який підтримує ISSRM за допомогою моделювання загроз, категоризації, відстежуваності, вираження потреби в безпеці, вираження вимог безпеки і пропозицій щодо контрзаходів для управління ризиками безпеки. Активи для системи електронної комерції можуть бути визначені з моделі бізнес-процесів системи. За допомогою цієї моделі ілюструються як бізнес-активи, так і системні активи неявно або явно, виконуючи вимоги ISSRM, пов'язані з активами. STRIDE використовується для виявлення загроз системним активам, дотримуючись моделі домену ISSRM для отримання оцінки впливу та ризиків. Процедура обробки ризиків STRIDE призводить до визначення вимог безпеки. Виявлені вимоги безпеки з використанням маркування STRIDE можуть бути застосовані до бізнес-процесів, щоб показати процеси, які потребують оптимізації та контрзаходів безпеки для управління ризиками. Ці вимоги безпеки запроваджують дії та контрзаходи, які ведуть до зменшення ризиків для безпеки. Аналіз витрат і вигод допомагає приймати рішення щодо пом'якшення ризиків, оскільки ресурси можуть бути недоступними для обробки всіх виявлених ризиків.

Адаптація цього підходу до інших сфер буде вигідною для дослідження ризику безпеки та впровадження менеджменту.

ВИСНОВКИ

Електронна комерція – це фінансові операції та операції, що здійснюються через Інтернет та приватні мережі зв’язку, під час яких купуються та продаються товари та послуги, а також грошові перекази. Слід зазначити, що поняття «електронна торгівля» та «електронна комерція» не тотожні – перше є невід’ємною частиною другого.

Витоки розвитку електронної комерції сягають початку 60-х років. XX століття, коли комп’ютери та системи зв’язку почали продавати авіаквитки, надавати низку банківських послуг (банківські системи VISA тощо), замовляти товари по телефону тощо. За такий короткий час ринок електронної комерції розвивався досить динамічно, що обумовлено стрімким зростанням кількості користувачів Інтернету, посиленням впливу соціальних мереж, динамічним розвитком електронних платіжних систем та електронних торгових платформ, переходом провідних гравців ринку в онлайн- середовище.

Аналіз впливу комбінації STRIDE та ISSRM на платіжний процес, об'єднані разом. Запропоновано підхід, орієнтований на загрози, що оцінюються експертами з безпеки, для управління ризиками безпеки. Запропоновано та проаналізовано підхід, заснований на оцінці загроз експертами з безпеки для управління ризиками безпеки. При цьому аналізується використання методу аналізу загроз безпеці - STRIDE для демонстрації інтенсивного аналізу загроз безпеці, який підтримує ISSRM, метод управління ризиками безпеки. STRIDE підтримує ISSRM за допомогою моделювання загроз, категоризації, відстежуваності, вираження потреби в безпеці, вираження вимог безпеки і пропозицій щодо контрзаходів для управління ризиками безпеки.

ПРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Афіногенов В. Б., Кабанов В. Ф. Основи електронної комерції: Навч. посібник: Наукова книга, 2008. 306 с.

2. Краус К.М., Краус Н.М., Манжура О.В. Електронна комерція та Інтернет-торгівля: навчально-методичний посібник. Київ: Аграр Медіа Груп, 2021. 454 с.

3. Мартовой А.В. Сущность и основные характеристики электронного бизнеса, электронной коммерции, электронного и интернет-маркетинга. *Культура народов Причерноморья*, 2004. 56 (1), С. 146-152.

4. Палеха Ю. І., Палеха О. Ю. Маркетинг інформаційних продуктів і послуг: Навч. посібник. К.: Видавництво Ліра-К. 2019. 480 с.

5. Boreyko N. M., Kovalenko, Yu. M. & Krasnova, T. D. *Taxation of e-commerce in Ukraine*: a monograph. (Series «Tax and Customs Affairs in Ukraine». Kyiv: Alerta, 2017. 357 p.

6. Nanehkaran Y. An Introduction To Electronic Commerce. *International Journal of Scientific & Technology Research*, 2 (4), 2013. P.190-193.

7. Summer A., Dunkan Gr. E-Commerce. New York: NYH Publishing, 1999. 427 p.

8. Chaffey D., Hemphill T., Edmundson-Bird D. Digital business and e-commerce management. Pearson UK, 2019. 297 p.

9. Korper S., Ellis J. The E-commerce Book: Building the E-empire. Elsevier, 2000. 359 p.

10. Green D., Hanbury M. If you shopped at these 14 stores in the last year, your data might have been stolen. Business Insider, 6. URL: https://www.businessinsider.com/ data-breaches-2018-4.

11. Matulevicius R., Norta A., Udokwu C., Noukas R. Security risk management in the aviation turnaround sector. *In International Conference on Future Data and Security Engineering. Springer*, Cham, 2016. P. 119–140.

12. Dubois E., Heymans P., Mayer N., Matulevicius, R., A Systematic Approach to Define ˇ the Domain of Information System Security Risk Management. *In: Intentional Perspectives on Information Systems Engineering, Springer,* 2010. P. 289–306.

13. Radack S. Managing information security risk: organization, mission and information system view. *National Institute of Standards and Technology*. No. ITL Bulletin March 2011. P. 459-472.

14. Janulevicius J. Method of Information Security Risk Analysis for Virtualized System (Doctoral dissertation, VGTU leidykla Technika). 2016. 378 p.

15. Li T., Horkoff J. Dealing with security requirements for socio-technical systems: A holistic approach. *In International Conference on Advanced Information Systems Engineering. Springer,* Cham, 2014. P. 285–300.

16. Fredriksen R., Kristiansen M., Gran B., Stølen K., Opperud T., Dimitrakos T. The CORAS framework for a model-based risk management process. *In:International Conference on Computer Safety, Reliability, and Security, Springer*, 2002. P. 94–105.

17. Alberts C., Dorofee A., Stevens J., Woody C. Introduction to the OCTAVE Approach. Carnegie-mellon University Pittsburgh PA Software Engineering Institute, 2003. 417 p.

18. Farquhar B. One approach to risk assessment. In: *Computers & Security*, 10(1), 1991. P. 21–23.

19. DCSSI Advisory Office. EBIOS: Expression of Needs and Identification of Security Objectives. Technical Report, Secretariat general de la defense nationale, Direction centrale de la securite des systemes d'information, 2010. 258 p.

20. De Risques M. H. D. A. MEHARI. Clusif, France. 2007. 392 p.

21. Chancellery A. F. Austrian IT Security Handbook, 2004. 468 p.

22. BSI Standard. 100-3. Risk Analysis Based On It-grundschutz-version, 2, 2008. 566 p.

23. Dalpiaz F., Paja E., Giorgini P. Security requirements engineering: designing secure socio-technical systems. MIT Press, 2016. 458 p.

24. Paja E., Dalpiaz F., Giorgini P. Managing security requirements conflicts in socio-technical systems. *In:International Conference on Conceptual Modeling, Springer*, 2013. P. 270–283.

25. Lund M. S., Solhaug B., Stølen K. The CORAS approach, 2011. 289 p.

26. Stølen K. CORAS A Framework for Risk Analysis of Security Critical Systems. *In: Supplement of the 2001 International Conference on Dependable Systems and Networks*, 2001. P. D4-D11.

27. Raptis D., Dimitrakos T., Gran B., Stølen K. The CORAS approach for model-based risk management applied to e-commerce domain. *In:Advanced Communications and Multimedia Security. Springer*, 2002. P. 169–181.

28. Stephens J., Valverde R. Security of e-procurement transactions in supply chain reengineering. *Computer and Information Science*, 6. 2013. P. 58-68.

29. Affia A.A.O. Security Risk Management of E-commerce Systems: Masters dissertation, 2018. 128 p.

30. Bresciani P., Perini A., Giorgini P., Giunchiglia F., Mylopoulos J. Tropos: An agentoriented software development methodology. *Autonomous Agents and Multi-Agent Systems*, 8(3), 2004. P. 203-236.

31. OMG Notation (bpmn) version 2.0. OMG Specification, *Object Management Group*, 2011. P. 22– 31.

32. Sindre G., Opdahl A. L. Eliciting security requirements with misuse cases. *Requirements engineering*, 10(1), 2005. P. 34–44.

33. Sindre G. Mal-activity diagrams for capturing attacks on business processes. *In: International working conference on requirements engineering: foundation for software quality*, 2007. P. 64-72.

34. Shostack A. Threat modeling: Designing for security. John Wiley & Sons, 2014. 468 p.

35. CAPEC. Common Attack Pattern Enumeration Classification. URL: https://capec.mitre. org.

36. Wichers D. Owasp top-10 2013. OWASP Foundation, 2013. 256 p.

37. Uzunov A. V., Fernandez, E. B. An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces*, 36(4), 2014. P. 734–747.

38. Ahmed N., Matulevicius R. Securing business processes using security risk-oriented patterns. *Computer Standards & Interfaces*, 36(4), 2014. P. 723-733.

39. Deng M., Wuyts K., Sc, Ariato R., Preneel B., Joosen W. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering*. 16, 2011. P. 3–32.

40. Liu Y., Man H. Network vulnerability assessment using Bayesian networks. In Data mining, intrusion detection, information assurance, and data networks security 2005. *International Society for Optics and Photonics*, 2005. Vol. 5812, P. 61-71.

41. CAPEC. Common Attack Pattern Enumeration Classification. URL: https://capec.mitre. org.

42. Stoneburner G., Goguen A., Feringa A. Risk management guide for information technology systems. NIST special publication, 2002. 800 p.

43. Uzunov A. V., Fernandez E. B. An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces*, 36(4), 2014. P. 734–747.

44. Howard M., Lipner S. The security development lifecycle. (Vol. 8). Redmond: Microsoft Press, 2006. 566 p.

45. Xu D., Nygard K. E. A threat-driven approach to modeling and verifying secure software. *In Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering*, 2005. P. 342–346.

46. Xu D., Nygard K. E. Threat-driven modeling and verification of secure software using aspect-oriented Petri nets. *IEEE transactions on software engineering*, 32(4), 2006. P. 265–278.

47. Xu D., Pauli J. Threat-driven design and analysis of secure software architectures. *Journal of Information Assurance and Security*, 1(3), 2006. P. 171–180.

48. Yanyan W. Research on e-commerce Security based on Risk Management Perspective. *International Journal of Security and Its Applications*, 8(3), 2014. P. 153-162.

49. Crowell A. A Survey of Access Control Policies. University of Maryland, 2011. 288 p.

50. Xin T., Xiaofang B. Online Banking Security Analysis based on STRIDE Threat Model. *International Journal of Security and Its Applications*, 8(2), 2014. P. 271-282.

51. Samarutel S. Matulevicius R., Norta A., Noukas R. Securing airline-turnaround processes using security risk-oriented patterns. In: *IFIP Working Conference on The Practice of Enterprise Modeling. Springer, Cham*, 2016. P. 209–224.

52. Here`s Why e-commerce growth can stay stronger for longer URL: https://www.morganstanley.com/ideas/global-ecommerce-growth-forecast-2022

53. Nina Taniguchi/May 2021 COVID changed the consumer journey, but what’s likely to stick? URL: https://www.thinkwithgoogle.com/consumer-insights/consumer-journey/covid-decision-journey/

54. Marketplaces URL:https://www.webreiltr.com/b/on-line-marketplaces

55. Global eCommerce sales growth (2021–2026). URL:https://www.oberlo.com/statistics/global-ecommerce-sales-growth

56. Michael Keenan Global Ecommerce Explained: Stats and Trends to Watch. URL: https://www.shopify.com/enterprise/global-ecommerce-statistics#10

57. mCommerce-forecast-2021 URL: https://www.emarket.com/content/mCommerce-forecast-2021

58. Simamkele Matuntuta 8 B2B Ecommerce Trends To Lock Your Eyes on in 2022. URL: https://www.plytix.com/blog/8-b2b-ecommerce-trends-to-lock-your-eyes-on-in-2022

59. Arnau Bages-Amat, Liz Harrison, Dennis Spillecke, and Jennifer Stanley New analysis makes it clear: For B2B sales, digital is the wave of the future. URL: https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/these-eight-charts-show-how-covid-19-has-changed-b2b-sales-forever

60. Future of Ecommerce. URL: https://www.shopify.com/research/future-of-commerce/future-of-ecommerce#Trend2

61. Voice assistant transaction values to grow by over 320% by 2023, but content libraries must expand. URL: https://www.juniperresearch.com/press/voice-assistant-transaction-values-grow-by-320

62. Кравець Т. Що таке маркетплейси, і на чому вони заробляють. URL: https://news.sap.com/ukraine/2017/05/what-is-marketplace/ (дата звернення: 18.11.2022).

63. Юдін А. Світовий e-commerce і m-commerce – статистика і факти електронної комерції 2020. URL: https://marketer.ua/ua/e-commerce-worldwide-statistics-facts/ (дата звернення: 18.11.2022).

64. Маркевич К. Куди йде електронна комерція. Мовою цифр / Центр Разумкова. URL: https://razumkov.org.ua/statti/kudy-ide-elektronna-komertsiia-movoiu-tsyfr (дата звернення: 16.11.2022).

65. Retailers Прогноз: у 2022 році на електронну комерцію буде приходитися 33% роздрібних продажів. URL: https://retailers.ua/news/menedjment/13199-prognoz-u-2022-rotsi-na-elektronnu-komertsiyu-bude-prihoditisya-33-rozdribnihprodajiv (дата звернення: 21.11.2022).

66. Zhiyong L., Zipei L. A blockchain-based framework of cross-border e-commerce supply chain. *International Journal of Information Management,* 52, 2020. P.102-122.

67. Офіційний сайт Державної служби статистики України URL: http://www.ukrstat.gov.ua (дата звернення 02. 12. 2022)

68. Yavors′kyy S., Berezans′kyy Y. Trendy elektronnoyi komertsiyi, vyklyky i mozhlyvosti. *Stalyy rozvytok – stan taperspektyvy. III mizhnarodnyy naukovyy sympozium*. L′viv-Slavs′ke, sichen′ 26-29. L′viv – Slavs′ke:Natsional′nyy universytet «L′vivs′ka politekhnika», 2022. P. 2015-2017.

69. Alexander I. F., Stevens R. Writing better requirements. Pearson Education. Breach Level Index, 2019. 427 p.

70. Davis A., Overmyer S., Jordan K., Caruso J., Ashi F., Dinh A., Kincaid G., Ledeboer G., Reynolds P., Sitaram P. and others. Identifying and measuring quality in a software requirements specification. *In:Proceedings First International Software Metrics Symposium,* IEEE, 2019. P. 141–152.

71. Mayer N., Dubois E., Matulevicius R., Heymans P. Towards a Measurement Frame-work for Security Risk Management. In MODSEC@ MoDELS. URL: http://ceur-ws.org/ vol-413/paper17.pdf.

72. CWE. Common Weakness Enumeration. A community-developed dictionary of software weakness types. URL: https://cwe.mitre.org/index.html.

73. Uzunov A. V., Fernandez E. B. An extensible pattern-based library and taxonomy of security threats for distributed systems. Computer Standards & Interfaces, 36(4), 2014. P. 734–747.