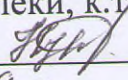


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет кораблебудування імені адмірала Макарова
Навчально-науковий інститут автоматики і електротехніки
Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних
технологій та інформаційної
безпеки, к.т.н., доцент
 С.М. Нужний
« 19 » 02 2024 р.

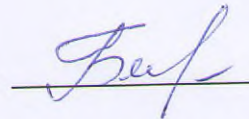
Кваліфікаційна робота
на правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА

**Побудова та дослідження моделей ефективності роботи електронного
магазину із забезпеченням інформаційної безпеки.**

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації,
автоматизація її обробки

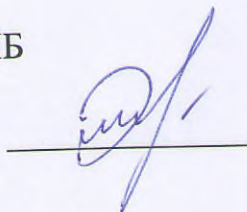
Виконав: студент 6 курсу групи 6366м
Безкоровайний Владислав Володимирович



Кваліфікаційна робота містить результати самостійного виконання
навчального завдання. Використання ідей, результатів і текстів інших авторів
мають посилання на відповідне джерело

Керівник:
д.т.н., професор кафедри КТІБ

Передерій Віктор Іванович



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ

Гарант освітньої програми, к.т.н.,
доцент, доцент кафедри КТІБ

 Турти М.В.

« 19 »  2024 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Безкоровайний Владислав Володимирович

Курс:6

Група: 6366мз

Ступінь вищої освіти: магістр

Галузь знань: 14 Електрична інженерія

Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»

Освітньо-професійна програма: Системи технічного захисту інформації,
автоматизація її обробки

1. Тема роботи: Побудова та дослідження моделей ефективності роботи електронного магазину із забезпеченням інформаційної безпеки.

Затверджена наказом НУК від « 14 » жовтня 2024 р. № 1075 - уч

2. Вихідні дані до роботи: Методи аналізу стратегії електронної комерції інтернет-магазину із забезпеченням інформаційної безпеки.

3. Перелік питань, які необхідно розробити:

1. Визначити основні особливості стратегії для інтернет-магазинів.
2. Визначити основні вимоги що пред'являються до електронної комерції із забезпеченням інформаційної безпеки.
3. Провести аналіз сучасного стану електронної комерції.
4. Визначити основні задачі та вимоги до функціонування інтернет магазинів.
5. Розробити та дослідити інформаційну та математичну моделі функціоналу інтернет-магазину.
6. Провести оцінку впливу основних факторів безпеки на ефективність роботи електронної комерції з використанням математичного апарату БМД.
7. Застосування методу шифрування RSA в системі онлайн магазину.

4. Терміни виконання завдання:

термін видачі завдання: « 04 » вересня 2024 р.
термін подання роботи: « 19 » грудня 2024 р.

6. План-графік виконання кваліфікаційної роботи

№ п/ п	Заходи	Дата		Готовність	Відмітка про виконання
		Навч. тиждень	Контрольна дата		
1.	Наукове стажування	1 - 8	25.10.2024	Звіт з наукового стажування	<i>вм</i>
2.	Організаційні збори	9	31.10.2024	Попередній варіант змісту КР	<i>вм</i>
3.	Рубіжний контроль	10	05.11.2024	Попередній варіант оглядових розділів	<i>вм</i>
4.	Рубіжний контроль	13	28-29.11.2024	1. Попередній варіант повної КР. 2. Попередній варіант презентації.	<i>вм</i>
5.	Рубіжний контроль	15	12.12.2024	Доповідь на 12-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПБТ-2024»	<i>вм</i>
6.	Перевірка на плагіат	15	12-13.12.2024	Електронний варіант кваліфікаційної роботи	<i>вм</i>
7.	КЕ на рівень « магістра »	16	17-18.12.2024	Здавання державного екзамену зі спеціальності на ступінь бакалавра	<i>вм</i>
8.	Кафедральний захист	16	19.12.2024	1. Оформлена КР (в форматі pdf) (передається студентом на кафедрі для внутрішньої рецензії). У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).	<i>вм</i>
9.	Подання документів на захист	16	20.12.2024	1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР. 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Електронний варіант та роздрукована презентація в кількості 5 примірників. 4. Електронний варіант КР на диску	<i>вм</i>
10.	Захист ДР	17	24,26,27, 28.12.2024	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.	<i>вм</i>

ПРИМІТКА: Завдання додається до виконаної роботи та подається до атестаційної комісії.

Керівник
д.т.н., професор кафедри КТІБ

В.І. Передерій
В.І. Передерій

Студент

В.В. Безкоровайний
В.В. Безкоровайний

АНОТАЦІЯ

У роботі досліджена проблема створення та аналізу стратегії електронної комерції. Проведено детальний аналіз основних проблем, пов'язаних із захищеністю інтернет-магазину, визначено ключові фактори впливу загроз на електронну комерцію. Зосереджено увагу на детальному аналізі сучасних методів та засобів для оцінки та підтримки захищеності інформаційних ресурсів електронних магазинів.

Проведено дослідження інформаційних потоків роботи інтернет магазину, та побудована Інформаційна та інформаційно-логічна моделі з урахуванням забезпечення інформаційної безпеки. Для забезпечення безпеки роботи інтернет магазину застосовано метод шифрування RSA.

Для дослідження і визначення впливових факторів конкурентоспроможності та оцінки рівня захищеності електронної торгівлі використані системний аналіз, графо-аналітичні методи Байєсівської мережі довіри та теорія експертних оцінок.

Використання теоретичних та практичних підходів допоможе вирішити завдання з оцінки підвищення ефективності і безпеки електронного магазину, зокрема при урахуванні їхнього рівня невизначеності та суб'єктивності.

Ключові слова: електронна комерція, інтернет-магазин, інформаційна модель, інформаційна безпека, методи шифрування, системний аналіз, графо-аналітичні методи, Байєсовська мережа довіри, теорія експертних оцінок, невизначеність, суб'єктивність.

ABSTRACT

The paper investigates the problem of creating and analyzing an e-commerce strategy. A detailed analysis of the main problems related to the security of an online store has been conducted, and key factors influencing the impact of threats on e-commerce have been identified. Attention is focused on a detailed analysis of modern methods and tools for assessing and maintaining the security of information resources of e-stores.

The paper studies the information flows of the online store, and builds an Information and Information-Logic model taking into account information security. The RSA encryption method is used to ensure the security of the online store.

To study and determine the influential factors of competitiveness and assess the level of security of e-commerce, system analysis, graph-analytical methods of the Bayesian trust network and the theory of expert assessments have been used.

The use of theoretical and practical approaches will help solve the problem of assessing the effectiveness and security of an e-store, in particular, taking into account their level of uncertainty and subjectivity.

Keywords: e-commerce, online store, information model, information security, encryption methods, system analysis, graph-analytic methods, Bayesian trust network, expert judgment theory, uncertainty, subjectivity.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД – База даних.

IoT – Інтернет речей(Internet of Things).

SSL/ITS – Протокол захищеного з'єднання / транспортний шар безпеки(Secure Sockets Layer / Transport Layer Security).

AES – Сучасний стандарт шифрування даних(Advanced Encryption Standard).

DoSS – Система захисту від відмов обслуговування(Denial of Service Security).

RSA – Алгоритм шифрування (Rivest-Shamir-Adleman).

ЕК – Стратегія Електронної Комерції.

SEO – Оптимізація пошукових систем(Search Engine Optimization).

eCommerce – Електронна комерція.

B2B/B2C – тип електронної комерції (Бізнес-до-бізнес/Бізнес-до-клієнта).

SHA – Криптографічний алгоритм для створення унікальних хеш-значень(Secure Hash Algorithm).

EDI – Електронний обмін даними(Electronic Data Interchange).

МСП – категорія підприємств за розміром(Малий та середній бізнес).

DSS – Система захисту(Data Security System).

БМД – Байесовська Мережа Довіри.

ЕЦП – Електронний цифровий підпис.

GUI – Графічний інтерфейс користувача(Graphical User Interface).

ЗМІСТ

ВСТУП	8
1. ОСНОВНІ ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ТА ПРОВЕДЕННЯ ОЦІНКИ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	
1.1 Правові основи безпеки та оцінки безпеки інформаційної інфраструктури України.	11
1.2 Загальні підходи до оцінки інформаційної захищеності об'єктів критичної інфраструктури.	13
1.3 Роль та значення електронної комерції інтернет-магазинів в сучасному суспільстві.	18
2. АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО СТРАТЕГІЇ ЕЛЕКТРОННОЇ КОМЕРЦІЇ	23
2.1. Аналіз та класифікація електронної торгівлі.....	23
2.2.Вимоги, що пред'являються до електронної комерції із забезпеченням інформаційної безпеки.....	29
2.3. Постановка задачі на дослідження та оцінки стратегії електронної комерції з забезпеченням комплексної інформаційної безпеки.....	35
3. ЗАСТОСУВАННЯ МЕТОДІВ М'ЯКИХ ОБЧИСЛЕНЬ ОЦІНКИ ЕФЕКТИВНОСТІ РОБОТИ ІНТЕРНЕТ ТОРГІВЛІ	39
3.1 Дослідження інформаційних потоків для підвищення ефективності роботи інтернет – магазину.....	39
3.2. Дослідження та аналіз оцінки критеріїв підвищення ефективності конкурентоспроможності електронного - магазину з урахуванням забезпечення інформаційної безпеки.....	43
3.3. Визначення та оцінка впливу основних факторів конкурентоспроможності електронної комерції з урахуванням забезпечення інформаційної безпеки.	51

3.4. Розробка та дослідження математичної моделі оцінки конкурентоспроможності електронної комерції з урахуванням забезпечення інформаційної безпеки.	56
4. ПРАКТИЧНА РЕАЛІЗАЦІЯ	65
4.1. Вибір методу шифрування в системі онлайн магазину.....	65
4.2 Алгоритм роботи методу шифрування RSA..	67
4.3. Застосування методу шифрування RSA у системах електронної комерції.	69
4.3.1. Робота протоколів SSL/TLS із використання алгоритму RSA.....	70
ВИСНОВОК	76
СПИСОК ЛІТЕРАТУРИ	77

ВСТУП

Сучасний ринок на сьогодні зумовлює складну систему господарювання, в якій тісно взаємодіють ринкові закономірності, численні регулюючі інститути (передусім державні) і масова свідомість. В наш час для торгівельних підприємств є актуальним надання значної уваги використанню Internet - торгівлі у зв'язку з оптимізацією торгівельної діяльності, зміною платоспроможного попиту, зростанням витрат на використання основних фондів торгівлі та на логістичні операції, підвищення розміру оплати праці торгово-операційного персоналу тощо. Internet-торгівля продає товар за допомогою електронних технологій [1].

Ще зовсім недавно інформаційні технології не грали такої важливої ролі для успіху бізнесу. Тепер, після вступу в нове тисячоліття та епоху розвитку Інтернету, відділити сам бізнес від інформаційних технологій практично неможливо.

Торгівля через Інтернет дозволяє істотно знизити вартість продукції, оскільки відпадають потреби в утриманні торгових площ, придбанні торгівельного обладнання, не потрібно утримувати торгівельний персонал тощо. Крім того, споживач у реальному масштабі часу може переглянути номенклатуру продукції, що реалізується, швидко знайти потрібний товар, вияснити його характеристики, ознайомитися з відгуками інших споживачів, обрати зручний спосіб і час доставки товару, провести платежі через Інтернет і т.д.

Успіх електронної комерції багато в чому залежить від того, як поставлена система доставки і розрахунків. Оплата товарів і послуг, запропонованих в Інтернеті, через традиційні банківські установи, що приймають оплату від громадян готівкою, може проходити із затримками. Зміцнення інфраструктури електронної комерції повинне супроводжуватися наведенням ладу в роботі структур, здійснюючу доставку і оплату. Форми

оплати в Інтернет - торгівлі можуть бути самими різними: готівкою, післяплатою при отриманні товару поштою, банківським переказом, поштовим переказом, пластиковою картою, електронними грошима (в цьому випадку магазин і покупець повинні бути зареєстровані в одній з існуючих систем цифрових платежів).

Актуальність теми :

Розвиток ринкових відносин та вдосконалення інформаційних технологій спричинили появу багатьох нових видів бізнесу, одним з яких є Інтернет-торгівля. Перетворення торкнулися як зовнішніх відносин між компаніями і їх партнерами або клієнтами, так і внутрішньої структури самих компаній. З'явилися не тільки нові напрями ведення бізнесу, але і принципово змінилися ті, що вже існують [2].

Стрімкий розвиток електронного обміну даними та глобальної мережі Інтернет радикально змінюють способи здійснення зовнішніх торгових операцій. Компаніям електронний простір пропонує новий інструмент маркетингу та середовище для ведення бізнесу, засіб зниження витрат на комунікації з клієнтами. Останні, в свою чергу, отримали нове інформаційне джерело про товари та послуги, нові шляхи задоволення своїх потреб, а також новий ефективний засіб комунікації, як з виробниками, так і між собою.

Застосування Інтернету дозволяє швидко і з незначними витратами виводити продукцію на національний і міжнародні ринки. Перед компаніями відкриваються можливості отримання додаткового доходу.

На сьогодні перед електронною комерцією стоять важливі завдання по забезпеченню захисту надійного функціонування та інформаційної безпеки, особливо в умовах постійних технологічних змін та росту кіберзагроз.

Протягом останніх років спостерігається важливий розвиток методів та стратегій забезпечення інформаційної безпеки електронних магазинів. Інтеграція новітніх технологій та підходів, таких як аналіз даних, машинне навчання та штучний інтелект, дозволяє забезпечити надійний захист та збереження конфіденційності даних клієнтів.

Тому з метою ефективного врахування невизначеності, складності та суб'єктивних аспектів у процесі розробки та оцінки стратегій в онлайн-торгівлі необхідно розробляти нові підходи з урахуванням забезпечення інформаційної та кібернетичної безпеки, які дозволять знаходити гнучкі та конструктивні рішення, необхідні для успішної роботи електронних підприємств у сучасних умовах.

Мета дослідження: Метою роботи є побудова та дослідження моделей оцінки ефективності роботи електронного магазину з урахуванням забезпечення комплексної інформаційної безпеки.

Завдання дослідження:

- Проаналізувати сучасні інформаційні технології ефективності функціонування електронної комерції із забезпеченням інформаційної безпеки.

- Розробити інформаційну та математичну моделі ефективності роботи електронного магазину з урахуванням забезпечення інформаційної безпеки з використанням сучасних методів інформаційних технологій.

- Провести дослідження побудованих моделей для оцінки ефективності роботи інтернет-магазину, із забезпеченням комплексної інформаційної безпеки.

Об'єкт дослідження: Методи аналізу ефективності функціонування електронної комерції із забезпеченням інформаційної безпеки.

Предмет дослідження: Теоретичні та практичні методи застосування теорії м'яких обчислень для побудови інформаційної та математичної моделей ефективності роботи електронного магазину з урахуванням забезпечення інформаційної безпеки.

Методи дослідження: Системний аналіз, графо-аналітичні методи Байесовської мережі довіри, теорія експертних оцінок.

Очікуваний результат: Отримані результати можуть бути використанні у структурах онлайн-торгівлі, для підвищення конкурентоспроможності та інформаційної безпеки інтернет магазинів.

1. ОСНОВНІ ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ТА ПРОВЕДЕННЯ ОЦІНКИ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Правові основи безпеки та оцінки безпеки інформаційної інфраструктури України.

Основні правові основи безпеки та оцінки безпеки інформаційної інфраструктури України визначені:

- Законом України про критичну інфраструктуру від 16.11.2021:

Цей Закон визначає правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. [1]

- Законом України про національну безпеку України від 24.11.2021:

Цей Закон визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз. Також цим Законом визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони. [2];

- Рішенням Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" та Указом Президента України про цю Стратегію від 26.08.2021 Стратегія ґрунтується на положеннях Конституції України, законів України "Про національну безпеку України" та "Про основні засади забезпечення кібербезпеки України", Конвенції про захист прав людини і основоположних свобод, Конвенції про кіберзлочинність,

Стратегії національної безпеки України, затвердженої Указом Президента

України від 14 вересня 2020 року № 392, Концепції боротьби з тероризмом в Україні, 16 затвердженої Указом Президента України від 5 березня 2019 року № 53, інших нормативно-правових актів. [3];

- Законом України Про основні засади забезпечення КБ від 15.12.2021:

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. [4];

- Законом України «Про інформацію» регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. [5]

- Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», де в статті 8 стверджують, що Інформація, яка є власністю держави, або інформація з обмеженим доступом, (вимога щодо захисту якої встановлена законом), повинна оброблятися із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. [6]

- «Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», що затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 п.16 та свідчать про те, що для забезпечення захисту інформації в системі створюється як комплексна система захисту інформації, яка призначається для захисту інформації від: витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій; несанкціонованих дій з інформацією, у тому числі з використанням

комп'ютерних вірусів; спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування. [7]

- Законом України «Про захист персональних даних» регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. [8]

- Законом України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. [9]

1.2 Загальні підходи до оцінки інформаційної захищеності об'єктів критичної інфраструктури.

В даний час існує понад 30 міжнародних стандартів типу ISO/IEC 27000, пов'язаних з інформаційною безпекою, які спільно опубліковані Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Зокрема:

- ISO 27001 – це міжнародний стандарт, розроблений Міжнародною організацією зі стандартизації, який описує, як управляти інформаційною безпекою в компанії. Остання версія цього стандарту була опублікована в 2013 році, і його повна назва на сьогодні

- ISO/IEC 27001:2013. Перша версія стандарту, опублікована в 2005 році, базувалася на Британському стандарті BS 7799-2;

- ISO/IEC 27004 містить рекомендації щодо оцінки інформаційної безпеки. Цей стандарт добре поєднується з ISO 27001, тому що пояснює, як визначити, чи досягла система управління інформаційної безпеки своїх цілей;

- ISO/IEC 27005 містить рекомендації для управління ризиками порушення інформаційної безпеки. Це дуже гарний додаток до стандарту ISO 27001, тому що містить деталі того, як здійснювати оцінку та обробку ризиків.

ISO 27005 з'явився на основі британського стандарту BS 7799-3. Та Українські Нормативні документи технічного захисту інформації: - НД ТЗІ 1.1-003-99 - НД ТЗІ 2.5-004- 99 - НД ТЗІ 2.5-005-99 Ці стандарти є обов'язковими, проте їх значимість у сучасному соціумі складно переоцінити. В основі, вони відображають особливості сучасного рівня інформаційних технологій, але не містять наскрізних шкал цінності та переліків вимог безпеки систем захисту інформації, що супроводжує цим об'єктам інфраструктури. Тому будь-який процес оптимізації з позицій захисту критично важливих об'єктів, від технології розробки до етапу кінцевої реалізації та подальшої експлуатації, бажано починати з експертної оцінки (ЕО) задіяних технічних, програмних та програмно-апаратних засобів захисту інформації (ЗЗІ), що супроводжує ці об'єкти інфраструктури. Реалізація останніх починається з побудови моделі пізнання гіпотетичних інформ-об'єктів з апіорним захистом від можливих кібератак і інцидентів. Від різноманітних загроз природного та штучного походження. Виправдано вважається, що основою забезпечення безпеки інформаційної системи є три складові у вигляді конфіденційності, цілісності, доступності, а процес успішного захисту інформації в інформаційній системі залежить від рівня розвитку апаратного забезпечення, програмного забезпечення та рівня комунікації забезпечення зв'язку.

Використані процедури (механізми) захисту від потенційних загроз поділяють на фізичний рівень захисту, на рівень захисту персоналу та організаційний рівень, а саме поняття «інформаційна безпека» вводять з погляду або діяльності, спрямованої на забезпечення захищеного стану об'єкта, у цьому значенні частіше використовується термін «захист інформації», або стану як якості певного об'єкта, як об'єкт може виступати і інформація, і дані, і ресурси автоматизованої системи, і сама автоматизована система, та інформаційна система підприємства, суспільства, держави. [10].

Очевидно, що дії кібер-зловмисників (хакерів) за допомогою шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на

виведення системи з ладу, як правило, забезпечується за допомогою різних типів мереж, серед яких найбільш бажаною є абстрактна мережева модель для комунікацій і розробки мережевих протоколів типу OSI [11]

Очевидно, що загрози виникають у разі наявності у систем захисту вразливостей, які можуть призвести до порушення безпеки. У свою чергу характер уразливості залежить від джерела виникнення, місця прояву в життєвому циклі КВО з підсистемами захисту, ступеня прояву потенційних ризиків у процесі експлуатації об'єкта, що охороняється, та СЗІ. Тому визначенню переліку загроз та побудові моделі порушника приділяється серйозна увага на такому обов'язковому етапі як побудова оцінної моделі не тільки запланованої системи захисту, а й безпосередньо СЗІ, завдяки яким може бути спровоковано та проведено успішну атаку на безпеку всієї кіберсфери.

Маючи правову базу, можемо визначитись з основними термінами та поняттями для подальшого дослідження поставленого завдання.

Отже, якщо «інформаційна безпека» - це стан захищеності інформаційного середовища, то захист інформації - являє собою діяльність із запобігання витoku інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, тобто процес, спрямований на досягнення цього стану. При цьому розрізняють інформаційну безпеку організації, як стан захищеності інформаційного середовища організації, що забезпечує її формування, використання та розвиток та інформаційна безпека держави, як стан збереження інформаційних ресурсів держави та захищеності законних прав особи та суспільства в інформаційній сфері.

Найчастіше поняття «інформаційної безпеки» та «кібер-безпеки» використовують як синоніми, оскільки їх родовий зв'язок визначений через поняття «безпека». Проте, ці два терміни істотно помітні незалежно від використання терміна «безпека», яке грає чи не найголовнішу роль переважають у всіх життєвих процесах: біологічних, політичних, економічних, технічних, територіальних та інших. Тому слід акцентувати на правильне використання цього поняття та його похідних відповідно до їх призначення. Так, наприклад, у

[12] озвучено, що «безпека – галузь науки, що вивчає природні, техногенні, соціальні, економічні та інші процеси освіти, розвитку та взаємодії суб'єктів, об'єктів довкілля та їх комбінацій з метою виявлення джерел небезпек, визначення їх характеристик та формування законів та інших нормативних актів, що встановлюють поняття, вимоги, рекомендації та методики, виконання яких має гарантувати захищеність інтересів окремої особи та суспільства загалом від усіх виявлених та вивчених джерел небезпеки». У такому разі за аналогією слідує, що кібербезпека - розділ безпеки, що вивчає процеси формування, функціонування та еволюції кібероб'єктів, з метою виявлення як джерел кібернебезпеки, які можуть завдати їм шкоди, так і формування законів та інших нормативних актів, що регламентують терміни, вимоги, правила, рекомендації та методики, виконання яких має гарантувати захищеність кібероб'єктів від усіх відомих та вивчених джерел кібернебезпеки. Безпосередньо поняття захищеності об'єкта вказує на його захист від зовнішніх джерел небезпеки, у той час як безпека об'єкта – це внутрішня властивість об'єкта не бути джерелом небезпеки для навколишнього середовища. З таких позицій слід розрізняти ці два терміни:

«кібербезпека об'єкта» та «кіберзахищеність об'єкта», що відповідають в англійській інтерпретації «cyber safety object» та «cyber security object». Звідси - кіберзахищеність об'єкта - властивість об'єкта, що характеризує його зовнішні можливості запобігати утворенню збитків від кібератак або обмежувати його величину допустимими нормами. Тоді «інформаційна захищеність це захист конфіденційності, цілісності та доступності інформації», а інформаційну безпеку слід розглядати як забезпечення стану захищеності:

- особи, суспільства, держави від впливу недоброякісної інформації;
- інформації та інформаційних ресурсів від неправомірного та несанкціонованого впливу сторонніх осіб;
- інформаційні права і свободи громадянина і людини [13].

Зазвичай СЗІ КВО поєднують засоби отримання, доставки, зберігання та безпосереднього захисту задіяної інформації. Остання, з погляду [14] – це сенсове у фундаменті буття, що забезпечує достовірність і цілісність у

пізнавальної, науково-практичної, виробничої, побутової та інших сферах життєдіяльності людини. Все інше, у тому числі і будь-яке її спотворення, свідоме чи ненавмисне, доцільно розглядати як повідомлення, яке може бути помилковим.

Все викладене вище дозволяє судити про багатокритеріальний характер безпеки життєдіяльності суспільства та його соціуму.

Згідно Закону України «Про основні засади забезпечення кібербезпеки України» [4] прийнято розуміти, що:

- кіберінцидент - подія або ряд несприятливих подій ненавмисного характеру, природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору, або таких, що мають ознаки можливої потенційної кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем, у тому числі зриву або блокування роботи системи, або управління її ресурсами, ставлять під загрозу безпеку електронних інформаційних ресурсів;

- кібербезпека – це захищеність життєво-важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

- кібератака - спрямовані дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій, включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання, та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються в комунікаційних або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних або технологічних систем; використання

комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

- кіберпростір – це середовище, яке надає можливості для здійснення комунікацій або реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних.

При цьому Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, де безпосередньо підприємства, установи та організації, які віднесені до об'єктів критичної інфраструктури, безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки [4].

1.3 Роль та значення електронної комерції у торговельній діяльності сучасного суспільства.

Існує багато визначень основних понять „електронна комерція”, „Інтернет-комерція”, а також близьких до них понять „електронна торгівля” та „Інтернет-торгівля”. Кожний автор відповідно до своєї професійної підготовки та накопиченого досвіду укладає в ці поняття свій зміст. Виникнення „електронної комерції” як науки було пов'язано з введенням в обіг нових термінів, категорій та понять, таких як: електронний магазин, електронна торгівля, електронний аукціон, електронна вітрина, електронні гроші, електронні платіжні системи, електронний цифровий підпис [3].

Інтернет-торгівля - це частина електронної комерції, причому дуже бурхливо розвиненої. Під цим поняттям мається на увазі комерційна діяльність

в мережі, коли процес покупки-продажу товарів і послуг (весь цикл комерційної-фінансової транзакції або її частина) здійснюється електронним чином з використанням телекомунікаційних мереж та електронних фінансово-економічних інструментів за допомогою реклами та розповсюдження товарів та послуг в мережі Інтернет. Торговельні операції через Інтернет можуть здійснювати багато організацій і виробники товарів-послуг, і дистриб'ютори, і роздрібні торгові компанії [4].

При цьому спосіб оплати не має значення: розрахунки за покупку можуть здійснюватися навіть готівкою. Цінність електронної торгівлі для покупців полягає в тому, що вона значно економить час покупця на пошук і купівлю потрібного йому товару.

Популярність торгівлі товарами через Інтернет неухильно зростає. Така торгівля вигідна і продавцям, і покупцям. Продавці за рахунок економії на торгових площах мають можливість запропонувати покупцям вигідніші ціни в порівнянні зі звичайними магазинами. А покупцеві для здійснення покупки не потрібно навіть виходити з дому. Достатньо кілька разів клацнути комп'ютерною мишею по екрану монітора, і вибраний товар буде доставлений прямо на будинок.

На сьогодні розбудова інформаційного суспільства в Україні вимагає прискорення процесів інформатизації всіх сфер виробничо-господарської діяльності, пришвидшення темпів створення національної інформаційної інфраструктури ринку електронних послуг, завдяки чому телекомунікації, апаратно-програмне забезпечення, автоматизовані інформаційні системи, глобальна мережа Internet, інформація та знання повинні стати основними засобами виробництва.

Електронна комерція здійснює суттєвий вплив на всі види економічної діяльності. Основними завданнями щодо розвитку національної складової мережі Internet і забезпечення широкого доступу до неї в Україні є:

- 1) створення в найкоротші терміни належних економічних, правових, технічних та інших умов для забезпечення широкого доступу громадян,

навчальних закладів, наукових та інших установ і організацій всіх форм власності в мережі Internet;

2) розширення й удосконалення надання в мережі Internet об'єктивної політичної, економічної, правової, екологічної, науково-технічної, культурної та іншої інформації про Україну, її бізнес, постійне удосконалення способів подання такої інформації;

3) забезпечення конституційних прав людини і громадянина на вільне збирання, зберігання, використання і поширення інформації, свободу думки і слова, вільне вираження своїх поглядів і переконань;

4) забезпечення державної підтримки розвитку інфраструктури надання інформаційних послуг через мережу Internet;

5) створення умов для розвитку підприємницької діяльності і конкуренції у сфері використання каналів електронного зв'язку, створення можливостей для задоволення на пільгових умовах потреб у послугах навчальних закладів, наукових установ і організацій, установ охорони здоров'я;

6) розвиток і впровадження сучасних ІКТ у систему державного управління, фінансову сферу, підприємницьку діяльність, освіту;

7) розв'язання завдань щодо гарантування інформаційної безпеки держави, недопущення поширення інформації, забороненої законодавством;

8) удосконалення правового регулювання діяльності суб'єктів електронної економічної діяльності, виробництва, використання, поширення та зберігання електронних інформаційних продуктів, захисту прав на інтелектуальну власність, посилення відповідальності за порушення встановленого порядку доступу до інформаційних ресурсів всіх форм власності, за навмисне розповсюдження комп'ютерних вірусів.

Є державні заходи щодо просування стосовно розбудови інформаційного суспільства, прикладом яких слугує проект "Україна - розвиток через Internet" за підтримки Міжнародного банку реконструкції і розвитку [5].

Основною метою цього проекту є підтримка уряду України в підвищенні ефективності прийняття рішень, стимулювання розвитку інформаційного

сектору економіки і зміцнення громадянського суспільства з використанням ІКТ.

Реалізація проекту передбачає такі етапи його виконання:

1) електронний уряд - впровадження моделей електронної закупівлі товарів/послуг і електронного документообігу на центральному і регіональному рівнях;

2) електронний бізнес - створення технологічної інфраструктури та нормативно-правової бази, що дасть змогу легалізувати інтерактивні операції в мережі Internet в Україні;

3) електронна взаємодія держави та громадськості - розробка моделей та інструментів для залучення громадськості у процесах управління державою.

Ринок електронної комерції має великий потенціал в Україні. Важлива роль у зв'язку з цим покладається на виконання державної програми "Електронна Україна", яка здебільшого має декларативний характер.

Залучення інвестицій та наявність сприятливого інвестиційного клімату, підвищена увага з боку уряду до інтелектуального і наукового потенціалу мають сприяти розвитку ІКТ та становленню інформаційної економіки.

ІКТ-модернізація українських підприємств є безповоротним процесом, пов'язаним з переходом промислової економіки на електронні способи взаємодії.

Для того, щоб повсюдно впроваджувати системи електронної комерції, необхідно підвищити рівень автоматизації виробничих і торговельних підприємств, а також якість телекомунікацій, посилити безпеку передачі та обробки даних, створити прийнятну нормативно-правову базу електронних операцій.

На сьогодні найважливішими вимогами до систем електронної комерції є:

Кібербезпека: Зростання кількості онлайн-транзакцій підвищує зростання загроз кібербезпеці. Атаки з боку хакерів, фішингові атаки, витоки даних та поширення зловмисного коду (вірусів) - усе це може негативно

вплинути на сферу електронної комерції. Щоб захистити клієнтів і зберегти довіру споживачів компанії повинні інвестувати у ефективні заходи кібербезпеки, такі як шифрування даних, двофакторна аутентифікація та постійний моніторинг безпеки.

Інформаційна безпека: Через те, що електронна комерція збирає великі обсяги особистих даних про користувачів, такі як адреси, кредитні картки, історії покупок, тощо. Збереження та конфіденційність даних є критично важливим завданням. Розкриття або неправомірний доступ до особистих даних може призвести до серйозних порушень приватності, втрати довіри споживачів та навіть матеріальних збитків.

Ці тенденції свідчать про актуальність дослідження та аналізу причин зниження рівня ефективності в електронній комерції. Для підвищення результативності інтернет-магазину в умовах сповільнення розвитку електронної комерції, власникам бізнесу може бути корисно проводити аналіз цих факторів, вдосконалювати стратегії маркетингу, адаптувати асортимент товарів та послуг до потреб ринку та залучати клієнтів шляхом інновацій та персоналізації.

Висновки до першого розділу. У даному розділі розглянуті основні особливості організації та проведення оцінки захищеності об'єктів критичної інфраструктури. Наведені правові основи безпеки та оцінки безпеки інформаційної інфраструктури України.

Досліджена проблема створення та аналізу стратегії електронної комерції. Проведено детальний аналіз основних проблем, пов'язаних із захищеністю інтернет-магазину, визначено ключові фактори впливу загроз на електронну комерцію. Зосереджено увагу на детальному аналізі сучасних методів та засобів для оцінки та підтримки захищеності інформаційних ресурсів електронних магазинів.

2. АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО СТРАТЕГІЇ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

2.1 Аналіз та класифікація електронної торгівлі.

Електронна торгівля включає купівлю продаж товарів та послуг, надання інформації, інформаційне обслуговування споживачів до і після факту продажу, електронне бізнес співробітництво, забезпечує підвищення продуктивності всередині бізнес організацій тощо. У країнах Західної Європи вона використовується паралельно з фізичними бізнес процесами, а деякі компанії повністю переводять деякі бізнес функції на електронну основу, чим автоматизують важливі процеси і мінімізують людське втручання в них, що, у свою чергу, значно покращує якість інформації.

Еволюція форм електронної торгівлі проходила природнім шляхом. Продуктивними силами, які стимулювали їх розвиток, були сучасні досягнення у впровадженні нових інформаційних і комунікаційних технологій, розвиток програмного забезпечення, необхідність у швидкості обміну інформацією та у проведенні бізнес операцій. Спочатку торгові компанії створювали свої web-сайти, які наповнювали рекламними текстами, характеристиками продукції та їх фотографіями. У такий спосіб відбувалося впровадження замовлення та продаж товару за каталогами у середовищі Інтернет. Розміщення електронних каталогів у мережі замість публікації на папері і розсилання поштою спрощує їх відновлення, скорочує витрати і час доставки споживачам. З часом форми торгівлі у мережі змінювалися, але електронні каталоги стали основним інструментом розміщення інформації і у міжкорпоративній торгівлі. З удосконаленням технічних і програмних можливостей глобальної комп'ютерної мережі Інтернет виникають нові форми електронної торгівлі - інтернет магазин, електронні моли тощо. Доцільно зупинитися на характеристиці зазначених форм торгівлі. Вони можуть бути різні за рівнем складності: простий магазин (він включає у себе прайс лист, іноді з фотографією товару, пошукову систему та картку замовлень); магазин із системою внутрішнього адміністрування та віртуальним кошиком

споживача для оформлення замовлень. Основними відмінностями інтернет магазину від традиційного є активна взаємодія між продавцем і споживачем, велика кількість інформації й асортименту продукції та персоналізований підхід до кожного відвідувача.

Основними функціями електронного магазину є:

- 1) Надання якомога повнішої інформації про представлені товари і послуги;
- 2) прийом та обробка замовлень;
- 3) персоналізація відвідувачів; проведення платежів (за умови підключення до платіжної системи);
- 4) збір і аналіз статистичної інформації.

До найвідоміших світових інтернет магазинів належать Amazon (www.amazon.com) і BestBuy (www.bestbuy.com), українських - Azbooka (www.azbooka.com.ua), Bambook (www.bambook.com.ua) та ін [8].

Разом з традиційними секторами торгівлі "бізнес-бізнес" і "бізнес-споживач" в даний час на ринку послуг інтернет-торгівлі можна виділити сегменти pc-commerce, m-commerce, t-commerce. Основні форми інтернет-торгівлі реалізуються з використанням персональних комп'ютерів і мережі Інтернет: Інтернет-магазини, електронні торгові майданчики, електронні аукціони і Інтернет-біржі [9].

Основним моментом електронної торгівлі є просування товару в мережі Інтернет.

Просування товару, представляє собою цілий комплекс заходів, спрямованих на реалізацію товару (послуги). Воно включає в себе виробництво та використання інформації, рекламні заходи, індивідуальні консультації покупців та ін.

Способи просування товару (послуги) в мережі Інтернет включають в себе:

- 1) банерну рекламу;
- 2) офлайнову рекламу;

3) просування за допомогою реєстрації в пошукових системах і каталогах [11].

Для функціонування Інтернет-магазину необхідно мати як мінімум такі програмно-апаратні компоненти:

1. Web-вітрина - оформлений web-дизайнерськими засобами прайс-лист торгової компанії з можливістю прийому замовлень. Даний тип системи щонайкраще підходить для підприємств малого та середнього бізнесу. Web-вітрини не мають інтерактивних інтерфейсів управління і не пов'язані безпосередньо з бізнес-додатками компанії. Обмін даними з web-вітриною проводиться менеджерами вручну, за допомогою передачі файлів.

Електронна вітрина належить до простих організаційних форм електронної роздрібної торгівлі в системі B2C. Вона може мати самостійний характер або виступати складовою Інтернет-магазину. Електронна вітрина являє собою спеціалізований Web-сайт, який містить інформацію про перелік товарів, які пропонуються покупцям, та порядок розміщення замовлення на такі товари. Мета Web-вітрини у даному разі полягає у зборі попередніх замовлень для їх виконання у реальному режимі [12].

Схематично Web-вітрина зображена на рис. 2.1.



Рисунок 2.1 - Інтернет-вітрина.

Судячи з рис. 2. 1, Інтернет-вітрина є лише інструментом (засобом) для залучення покупців. Вона не може забезпечити повний цикл купівлі-продажу товару. Це завдання виконує Інтернет-магазин [13].

Інтернет-магазин - це спеціалізований Web-сайт, який забезпечує повний цикл купівлі-продажу товарів через Інтернет в інтерактивному режимі з використанням електронного каталогу. Отже, Інтернет-магазин забезпечує виконання таких операцій: ознайомлення, вибір товару, оформлення замовлення, проведення взаєморозрахунків, відстежування виконання замовлення.

Для функціонування Інтернет-магазину необхідно мати як мінімум такі програмно-апаратні компоненти:

- Інтернет-вітрину (фронт-офіс) на Web-сервері;
- електронні каталоги;
- електронну платіжну систему;
- інформаційну систему, інтегровану у фронт-офіс, тобто бек-офіс (склад, бухгалтерія, відділ доставки та ін.).

Інтернет-вітрина магазину має активний зміст. Вона може бути статичною на базі звичайних HTML-файлів або динамічною - з відображенням інформації з бази даних.

Інтернет-вітрина містить інформацію про назву, профіль, статус магазину, асортимент товарів, засоби платежів, знижки, порядку доставки товару, гарантії та Електронні каталоги являють собою довідники з пошуку товарів, послуг такими характеристиками: найменування; призначення; ціна; виробники; конкурентоспроможність тощо. Це, по суті, Web-сайт систематизованих товарів з доступною системою навігації.

2. Інтернет-магазин - повнофункціональна система ведення Інтернет-торгівлі з індивідуальними бізнес-схемами взаємодії зі споживачами. Інтернет-магазин містить, крім web-вітрини, всю необхідну бізнес-логіку для управління процесом Інтернет-торгівлі (бек-офіс). Гнучкість налаштувань бек-офісів Інтернет-магазинів і можливість швидкої розробки індивідуального

web-дизайну дозволяють використовувати Інтернет-магазин для організації торгівлі широким спектром товарів і послуг компаніям середнього та великого бізнесу.

Блок-схема Інтернет-магазину може бути подана таким чином (рис 2. 2) [14].

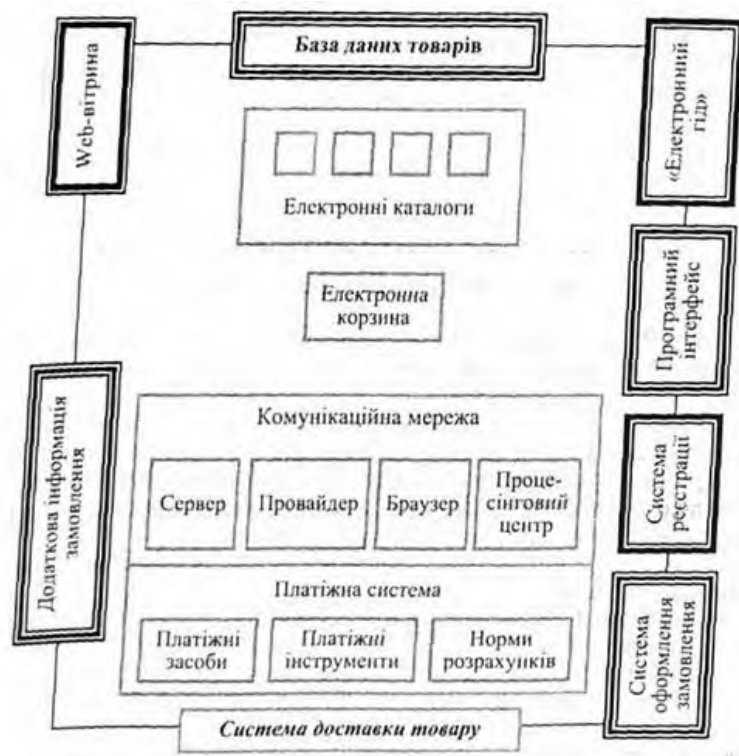


Рисунок 2.2 - Блок-схема Інтернет-магазину.

Залежно від асортименту, рівня електронних технологій, статусу, способу створення Інтернет-магазини можуть бути класифіковані у різних варіантах:

- 1) магазини універсальні, спеціалізовані і вузькоспеціалізовані;
- 2) магазини самостійні, підрозділ традиційного магазину;
- 3) магазин - власний, корпоративний, орендований [15].

Торговельний майданчик (торговельні ряди) являє частину Інтернет-торгівлі, де здійснюють купівлю-продаж одночасно численні покупці і продавці, використовуючи єдині служби, програми, апарати, каталоги та інші ресурси.

Існують три варіанти участі продавця в електронному торговельному ряду:

- 1) перший - розміщення прайс-листка продавця в каталозі торговельного майданчика з розбивкою на окремі групи товарів;
- 2) другий - пов'язаний з участю в торговельному ряді невеликого Інтернет-магазину і його поданням на сайті торговельного майданчика як цілісного об'єкта;
- 3) третій - передбачає оренду тематичного розділу каталогу, при цьому лише орендар має право представляти товари даної тематики або даного асортименту.

3. Торгова Інтернет-система (TIC) - складна і потужна система ведення торговельних операцій через Інтернет, в якій повністю інтегровані торгові процеси offline і системи online бізнесу компанії. Досягається це шляхом інтеграції зовнішнього Інтернет-магазину в бізнес-додатки, які є в компанії, з системами складського обліку, торгово-обліковими і бухгалтерськими системами, а для великих корпорацій - з ERP-системами, тобто TIC є Інтернет-магазин, бек-офіс якого повністю (в режимі реального часу) інтегрований в торговий бізнес-процес компанії.

4. Інтернет-аукціон - порівняно молода, але разом з тим перспективна організаційна форма у сфері електронної роздрібної торгівлі. Суть Інтернет-аукціону полягає в організації процесу роздрібної купівлі-продажу на базі сучасних інформаційних технологій! у публічній атмосфері з установленням кінцевої ціни на конкурентних засадах. Аукціонні торги проводяться за допомогою спеціального програмного забезпечення, що встановлюється на свиті організатора аукціону, тобто аукціонної фірми [16].

Залежно від технології проведення торгів аукціони можуть бути одночасних пропозицій, закритих пропозицій, очні і заочні, на підвищення стартової ціни (англійський) або на пониження ціни (голландський).

Схематично структура аукціону подана на рис. 2.3.



Рисунок 2.3 - Складові елементи електронного аукціону

Переваги електронного аукціону полягають у тому, що ця форма забезпечує динамічність, масштабність, конфіденційність, конкурентність у процесі електронної торгівлі.

2.2 Вимоги, що пред'являються до електронної комерції із забезпеченням інформаційної безпеки.

Щоб забезпечити успішне функціонування електронної комерції та відповісти на потреби сучасного споживача, необхідно враховувати ряд конкретних вимог при створенні та управлінні електронними торговими платформами [5].

- Перш за все, електронна комерція вимагає відповідності технічним стандартам і нормам. Системи повинні бути надійними, масштабованими та забезпечувати високий рівень безпеки. Це враховує застосування шифрування для захисту конфіденційної інформації користувачів та забезпечення стійкості до атак і вразливостей.

- Технічна інфраструктура є фундаментом електронної комерції, оскільки вона забезпечує надійність та стабільність роботи інтернет-магазину. Наявність потужного хостингу, програмного забезпечення для керування контентом і ефективних систем безпеки дозволяє забезпечити швидку та безпечну роботу сайту, що є критично важливим для задоволення потреб клієнтів та збільшення конверсії.

- Дизайн та користувацький досвід впливають на перше враження від інтернет-магазину і можуть визначити його успіх. Зручна навігація, естетичний дизайн та швидке завантаження сторінок допомагають залучити та утримати увагу користувачів, підвищуючи ймовірність їх перетворення в покупців.

- Безпека та конфіденційність є основними аспектами електронної комерції, оскільки клієнти передають свої особисті дані та здійснюють фінансові операції онлайн. Застосування шифрування, безпечних платіжних шлюзів і використання найкращих практик управління даними допомагає забезпечити захист від шахраїв та зловмисників.

- Обробка замовлень та логістика є важливим етапом в електронній комерції, оскільки швидка доставка та якісне обслуговування замовлень можуть впливати на задоволеність клієнтів і їх відношення до бренду. Чітке управління процесами доставки та ефективна система обробки замовлень допомагають забезпечити позитивний досвід покупців і зберегти їх лояльність.

- Не менш важливим є дотримання законодавства та етичних стандартів у сфері електронної комерції. Закони про захист особистих даних та правила збереження та обробки інформації вимагають уважного ставлення до приватності клієнтів.

- Безпека даних є критичним аспектом у віртуальному просторі, оскільки вона забезпечує захист конфіденційності та безпеку особистої інформації. Підприємства повинні використовувати шифрування та інші заходи захисту для забезпечення безпеки транзакцій та уникнення порушень безпеки даних

Шифрування — це метод перетворення відомих даних в незрозумілий, для особи яка не має спеціального ключа, код. Криптографічний ключ — це набір відомих математичних величин, погоджених як відправником, так і одержувачем [6].

Шифрування важливе у вимогах GDPR (Загального регламенту про захист даних), який регулює зберігання та обробку особистої інформації. Відповідно до GDPR, персональна інформація включає імена, адреси, електронні адреси та інші особисті дані. Вимоги GDPR вимагають від підприємств застосовувати ефективні заходи безпеки, такі як шифрування, для захисту особистих даних від несанкціонованого доступу та можливих порушень безпеки. Шифрування є ключовим елементом захисту корпоративної інформації та конфіденційних даних в сучасному бізнес-середовищі. Потенційні втрати або витoki конфіденційної інформації можуть призвести до серйозних наслідків для підприємства, зокрема втрати довіри клієнтів та санкцій від регулюючих органів. Тому важливо, щоб підприємства використовували технологію шифрування для захисту конфіденційної інформації та виконання вимог щодо захисту даних.

Найпоширеніші стандарти шифрування, які використовуються в електронній комерції, які представлені у таблиці 1.1, є: Secure Sockets Layer/Transport Layer Security(SSL/TLS), Advanced Encryption Standard(AES), Rivest-Shamir-Adleman(RSA), Secure Hash Algorithm(SHA) тощо.

Таблиця 2.1 – Стандарти захисту даних в Інтернеті.

Стандарт	Функція	Застосування
Secure http (S-HTTP)	Захист транзакцій в Web	Браузери, Web-сервери, програми для Інтернету
Secure Sockets Layer (SSL)	Захист пакетів даних на мережевому рівні	Браузери, Web-сервери, програми для Інтернету
Secure MIME (S / MIME)	Захист вкладень в електронні послання на різних платформах	Поштові програми з підтримкою шифрування та цифрового підпису RSA
Secure Wide-Area Networks (S / WAN)	Шифрування однорангових з'єднань між брандмауерами і маршрутизаторами	Віртуальні приватні мережі
Secure Electronic Transactions (SET)	Захист транзакцій з кредитними картами	Смарт-карти, сервери транзакцій, електронна комерція

Крім основних стандартів шифрування, інші заходи захисту даних в електронній комерції включають такі методи, як аутентифікація, авторизація, аудит, резервне копіювання, застосування фаєрволів, антивірусне програмне забезпечення та інші. Ці заходи спрямовані на контроль доступу до даних, виявлення та запобігання потенційним загрозам, а також на відновлення даних у разі їх втрати або пошкодження. Наприклад, для перевірки особи клієнта може використовуватись аутентифікація, а для надання доступу до певних функцій - авторизація. Аудит дозволяє відстежувати дії користувачів, а резервне копіювання забезпечує збереження даних у випадку відмови системи. Для захисту від кіберзагроз, ефективні методи включають створення складних паролів, використання біометричних ідентифікаторів, одноразових паролів та цифрових підписів, моніторинг системних логів, а також застосування антивірусного програмного забезпечення, мережевих екранів та фільтрів для блокування спаму. Всі ці заходи разом створюють багаторівневий захист, що зменшує ризик несанкціонованого доступу та інших форм кібератак.

Графічний інтерфейс користувача(GIU) - набір інструментів, які дозволяють користувачам взаємодіяти з веб-магазином, включаючи такі елементи, як меню навігації, кнопки дій, текстові поля, вибірки, графічні зображення, мультимедійний контент та інтерактивні функції. Важливо, щоб інтерфейс був інтуїтивно зрозумілим, не займав багато часу для того, щоб зробити заплановану покупку, і відповідав потребам користувачів, їхнім очікуванням і використанням пристроєм. Наприклад, інтерфейс веб-магазину має включати логічно структуровані категорії продуктів, візуально привабливі зображення, чіткі та інформативні описи продуктів, ефективні та безпечні методи оплати, а також засоби для зворотного зв'язку та підтримки.

Процес оформлення замовлення включає ряд етапів, які користувач має пройти для покупки товару чи послуги онлайн, від вибору продукту до

отримання підтвердження покупки. Це може охоплювати додавання товару до кошика, введення контактної інформації, вибір доставки та оплати, та отримання квитанції. Щоб забезпечити максимальну зручність та безпеку для користувача, процес повинен бути максимально спрощеним та інтуїтивно зрозумілим. Веб-магазин повинен надавати чіткі інструкції щодо оформлення замовлення, відображати статус замовлення на кожному етапі, дозволяти зміну або скасування замовлення, а також зберігати дані користувача для подальшого використання, забезпечуючи при цьому конфіденційність та безпеку інформації. Повинні бути доступні різноманітні варіанти доставки та оплати, щоб користувач міг обрати найзручніший для себе. Крім того, важливо мати чітку політику повернення товарів, щоб користувачі могли повертати або обмінювати товари у разі необхідності.

Стійкість до збоїв - це здатність системи функціонувати без перебоїв навіть у разі помилок, збоїв, атак або стихійних лих. Стійкість до збоїв може бути забезпечена активними методами (попередження збоїв за допомогою дублювання, кластеризації, балансування навантаження і т.д.) або пасивними методами (відновлення після збоїв за допомогою резервного копіювання, відновлення системи, перезапуску). Наприклад, онлайн-магазин повинен мати стійку до збоїв систему, щоб уникнути втрати інформації, функціональності або доступу до продукції чи послуг, а також для швидкого відновлення роботи в разі непередбачуваних ситуацій.

Масштабування - це можливість системи адаптуватися до збільшення обсягу користувачів, операцій, інформації, можливостей і так далі, зберігаючи при цьому ефективність, якість і безпеку. Масштабування може бути досягнуто шляхом вертикального розширення (підвищення характеристик окремих елементів, таких як ЦП(центральный процесор), пам'ять, диск та інше) або горизонтального розширення (додавання більшої кількості елементів, таких як сервери, бази даних, мережі і т.д.). Наприклад, онлайн-магазин повинен мати масштабовану архітектуру, щоб витримувати

сплески попиту на продукцію чи послуги, а також для розширення свого асортименту та можливостей.

Вимоги до інформаційної безпеки в електронній комерції охоплюють ряд стандартів та практик, спрямованих на захист даних та систем від несанкціонованого доступу та інших кіберзагроз. Серед основних вимог до проведення комерційних операцій – конфіденційність, цілісність, аутентифікація, авторизація, стійкість до кібератак, гарантії та збереження таємниці.

Перші чотири критерії інформаційної безпеки забезпечуються за допомогою програмного забезпечення та апаратних рішень, тоді як здійснення останніх двох – забезпечення гарантій та збереження конфіденційності – залежить не тільки від технічних засобів, але й від відповідальності індивідуальних осіб та організацій, а також від дотримання законодавства, яке захищає споживачів від потенційного обману. У фізичному світі ми приділяємо багато уваги захисту від фізичних загроз, тоді як у сфері електронної комерції необхідно зосередитися на захисті інформації, комунікацій та фінансових операцій. Працюючи з мережевими системами, такими як Інтернет та Інтранет(приватна комп'ютерна мережа для внутрішнього використання в одній організації), важливо пам'ятати про різноманітні загрози, такі як:

- Навмисне перехоплення, читання або зміна даних;
- Навмисне неправильне представлення користувачами своєї особи;
- Несанкціонований доступ користувачів до мережі, що не призначена для їх використання.

Стійкість до кібератак - це комплексна властивість інформаційних систем, яка забезпечує захист від різноманітних кіберзагроз, таких як віруси, фішинг, DDoS-атаки та інші. Вона включає в себе заходи як технічного, так і організаційного характеру: від файрволів, антивірусів і шифрування даних до багаторівневої аутентифікації, регулярних оновлень безпеки та навчання персоналу. Ефективна стійкість до кібератак також

передбачає створення резервних копій даних для швидкого відновлення системи після можливих інцидентів, забезпечуючи надійність та доступність інформаційних ресурсів.

2.3 Постановка задачі на дослідження та оцінки стратегії електронної комерції з забезпеченням комплексної інформаційної безпеки.

Оцінка ефективності стратегії електронної комерції включає аналіз досягнень у порівнянні з поставленими цілями, виявлення сильних сторін та аспектів для покращення. Важливо враховувати ринкові дані, такі як зростання обсягу ринку електронної комерції, що допомагає прогнозувати майбутні тренди та планувати стратегічні кроки. Наприклад, згідно з даними, обсяг ринку електронної комерції в Україні зростає, особливою популярними категоріями є хобі, електроніка, мода, меблі, товари для догляду, домашні товари та продукти харчування. Така інформація може бути корисною для оптимізації маркетингових зусиль та підвищення конкурентоспроможності.

Основними вимогами задачі оцінки ефективності на покращення рівня безпеки електронного магазину полягає в аналізі і оцінці його ефективності та рівня інформаційної безпеки для збільшення прибутку, залучення та задоволення клієнтів та масштабування.

Для цього необхідно виконати наступні етапи:

- Виявлення цільової групи споживачів, розподіл ринкових сегментів та визначення унікальних конкурентних переваг є ключовими для успіху в електронній комерції.

Основні категорії товарів, які користуються популярністю в онлайн-продажах, включають захоплення, електроніку, моду, меблі, побутову техніку, продукти особистої гігієни, домашні товари та продовольчі товари. Ринкове сегментування може бути засноване на таких параметрах, як місцезнаходження, вікова категорія, стиль життя, поведінкові фактори та особисті потреби. Ключові переваги електронної комерції включають

широкий асортимент, зручність і швидкість доставки, доступні ціни, гнучкість у способах оплати, можливість порівняти продукти та прочитати відгуки, а також використання передових технологій, таких як мобільні застосунки, соціальні мережі, штучний інтелект, VR та AR.

- Розробка маркетингової стратегії для електронної комерції включає аналіз ринку та аудиторії, вибір каналів просування, як SEO та соціальні медіа, та створення унікальної пропозиції цінності. Важливо враховувати ринкові тенденції, споживацькі переваги, а також конкурентну ситуацію. Ефективний бренд має бути запам'ятовуваним, з чіткою ідентичністю та відповідати емоційним потребам клієнтів.

- Моніторинг та аналітика в електронній комерції є важливими для оцінки ефективності маркетингу, розуміння поведінки користувачів та фінансових показників. Використання інструментів як Google Analytics, Facebook Pixel та інші, дозволяють відстежувати ключові показники ефективності, такі як відвідуваність, конверсії, та доходи, що допомагає виявити сильні сторони та аспекти для оптимізації.

- Аудит безпеки є критично важливим для ефективності інтернет-магазину, оскільки він допомагає забезпечити захист конфіденційної інформації клієнтів та компанії. Він включає в себе:

Оцінку потенційних загроз для інформаційних активів, що можуть призвести до втрати даних або фінансових збитків;

Виявлення вразливостей у системі захисту даних, які можуть бути використані зловмисниками;

Надання пропозицій щодо зміцнення інформаційної безпеки, включаючи технічні та організаційні заходи;

Переконавання в тому, що інтернет-магазин дотримується відповідних законів та стандартів, таких як GDPR [29].

Аудит безпеки допомагає підтримувати цю довіру, знижуючи ризик витоку даних та інших безпекових інцидентів, які можуть негативно вплинути на репутацію та фінансове становище компанії.

В результаті проведеного аналізу було виявлено кілька ефективних методів для збільшення лояльності клієнтів в інтернет-магазині. Ці методи включають використання програм лояльності, персоналізацію, розсилки через електронну пошту, активну присутність у соцмережах, співпрацю з інфлюенсерами, використання гейміфікації, випуск подарункових карток, проведення розіграшів та надання подяк.

Для підвищення рівня конкурентоспроможності інтернет торгівлі з забезпеченням комплексної інформаційної безпеки пропонується вирішення наступних задач:

- Регулярні оновлення всієї системи та програмне забезпечення, щоб запобігти використанню відомих вразливостей.
- Використання надійних паролів та багатофакторної аутентифікації. Також важливо регулярно оновлювати паролі користувачів і працівників, які відповідають за фронтенд інтернет-магазину.
- Шифрування даних, що передаються та зберігаються, особливо платіжної інформації та персональних даних користувачів.
- Встановлення та налаштування брандмауера та антивірусного програмного забезпечення для захисту від шкідливих програм та атак.
- Використання систем моніторингу та виявлення вторгнень для виявлення та реагування на підозрілу активність.
- Створення регулярних резервних копій важливих даних для відновлення після можливих інцидентів безпеки.
- Розробка чіткої політики безпеки та проведення регулярних тренінгів для персоналу щодо кращих практик безпеки.
- Дотримання міжнародних стандартів безпеки, таких як PCI DSS для платіжних систем, може допомогти забезпечити високий рівень захисту.

Для визначення та оцінки впливових факторів на ефективність та безпеку інтернет торгівлі, необхідно вирішити наступні питання:

- Аналіз підходів до стратегії електронного-магазину.

- Аналіз проблемної області, вивчення існуючих рішень, визначення цілей та обмежень проекту.
- Проведення системного аналізу в дослідженні та побудові моделей інтернет-магазину, включаючи розробку інформаційної та математичної моделі функціоналу.
- Реалізація програмного коду, який дозволить зашифрувати особисті дані користувачів інтернет-магазину.

Даний аналіз є важливим для розуміння та підвищення рівня безпеки в електронній комерції, що в свою чергу сприяє підвищенню довіри користувачів та успішному функціонуванню електронних магазинів.

Висновки до другого розділу. У даному розділі проведений аналіз та класифікація електронної торгівлі та сучасних підходів до стратегії електронної комерції. Розглянуті вимоги, що пред'являються до електронної комерції із забезпеченням інформаційної безпеки.

Для підвищення рівня конкурентоспроможності інтернет торгівлі з забезпеченням комплексної інформаційної безпеки запропоновано підхід та вирішення основних задач. Даний підхід є важливим для розуміння та підвищення рівня безпеки в електронній комерції, що в свою чергу сприяє підвищенню довіри користувачів та успішному функціонуванню електронних магазинів.

У розділі також визначена постановка задачі на дослідження та оцінки стратегії електронної комерції з забезпеченням комплексної інформаційної безпеки.

РОЗДІЛ 3. ЗАСТОСУВАННЯ МЕТОДІВ М'ЯКИХ ОБЧИСЛЕНЬ ОЦІНКИ ЕФЕКТИВНОСТІ РОБОТИ ІНТЕРНЕТ ТОРГІВЛІ

3.1 Дослідження інформаційних потоків для підвищення ефективності роботи інтернет – магазину.

Інформаційна модель роботи інтернет – магазину (рис. 3.1) представляє собою набір даних, які визначають структуру, функціональність, процеси та взаємодії всередині інтернет-магазину, створеного для проведення електронних комерційних операцій.

Класична структурна схема інтернет торгівлі

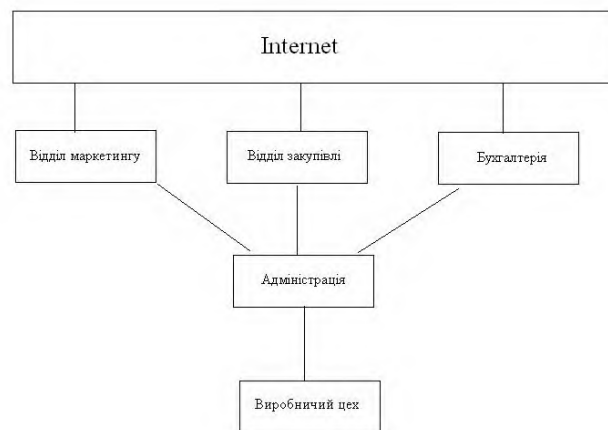


Рисунок 3.1- Інформаційні потоки

В процесі роботи Інтернет – магазину функціонують наступні інформаційні потоки:

- ведення обліку проданих товарів;
- ведення обліку зареєстрованих покупців;
- ведення обліку найбільш купованих товарів;
- список зареєстрованих користувачів;
- списки замовлень та їх стан;
- списки відгуків та коментарів;
- списки замовлень з найбільшим попитом;

- звіти продажів.
- інформація електронного кошика.
- ведення обліку зареєстрованих покупців.

Для визначення та оцінки стану інформаційної завантаженості побудуємо граф-схему циркулюючих інформаційних потоків інтернет – магазину. Схематичне представлення внутрішньої інформаційної моделі складається з:

Таблиця 3.1 - Інформаційні потоки між відділами

Відділ маркетингу	1
Відділ постачань	2
Автоматизоване робоче місце 1	3
Головний бухгалтер	4
Помічник головного бухгалтера	5
Адміністрація	6
Автоматизоване робоче місце2	7
Автоматизоване робоче місце3	8
Пункт реалізації	9
Сервісний центр	10

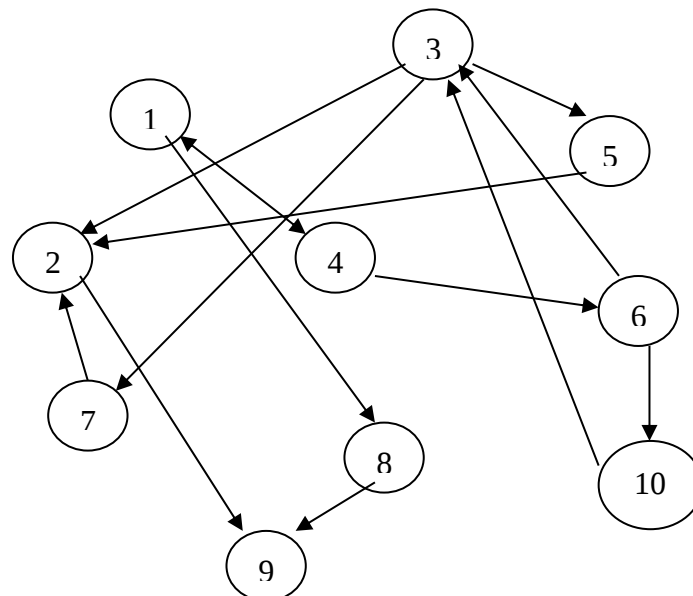


Рисунок 3.2 – Неупорядкована граф-схема інформаційного потоку.

Побудова матриці складності здійснюється по формулах:

$$I_0 = a \quad (i=1, n); \quad (3.1)$$

$$I_1 = I_0 - \sum a, \quad a=0; \quad (3.2)$$

$$I_k = I_{k-1} - \sum a, \quad a=0; \quad (3.3)$$

$$I_n = 0; \quad (3.4)$$

Таблиця 3.2 – Матриця складності.

	1	2	3	4	5	6	7	8	9	10
1				1				1		
2									1	
3		1			1		1			
4	1					1				
5		1								
6			1							1
7		1								
8									1	
9										
10			1							

На підставі матриці складності виявимо найбільш оптимальний розподіл інформаційних потоків і побудуємо перетворену схему графа показану на рисунку 3.3.

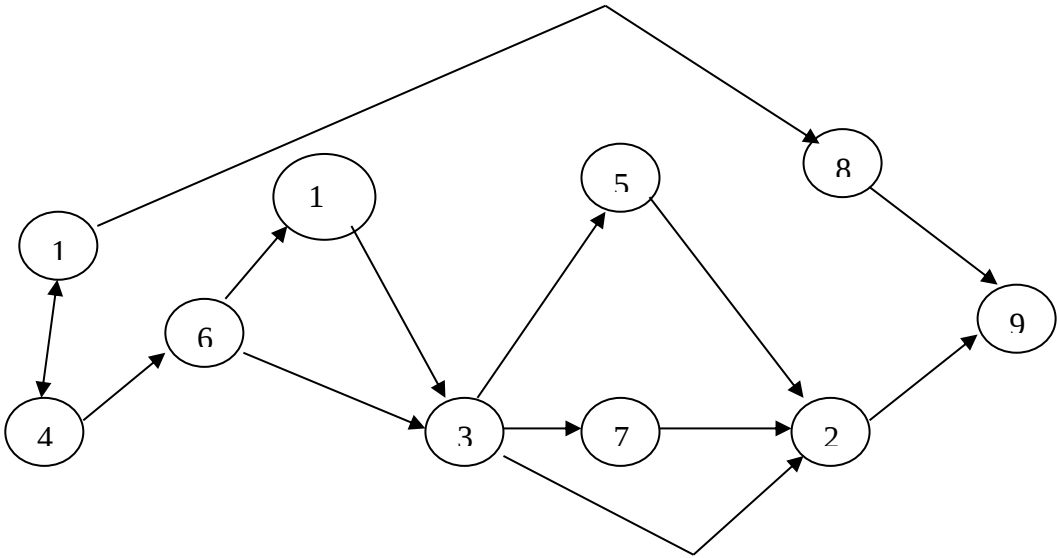


Рисунок 3.3 - Мінімізована упорядкована граф-схема інформаційного потоку.

У приведених рисунках (3.2,3.3) інформаційні потоки характеризуються: об'ємом переданої інформації (W,біт); часу заповнення одного документу (t,c); кількістю заповнених документів протягом робочого дня (λ ,шт); періодом заповнення загальної кількості документів (T,шт/кварт).

Для повного представлення інформаційної моделі електронної комерції побудована концептуальна схема бази даних, яка охоплює ключові елементи та їхні взаємозв'язки у системі [31].

Інформаційна модель бази даних електронного комерційного магазину може складатися з наступних компонентів (рис. 3.4):

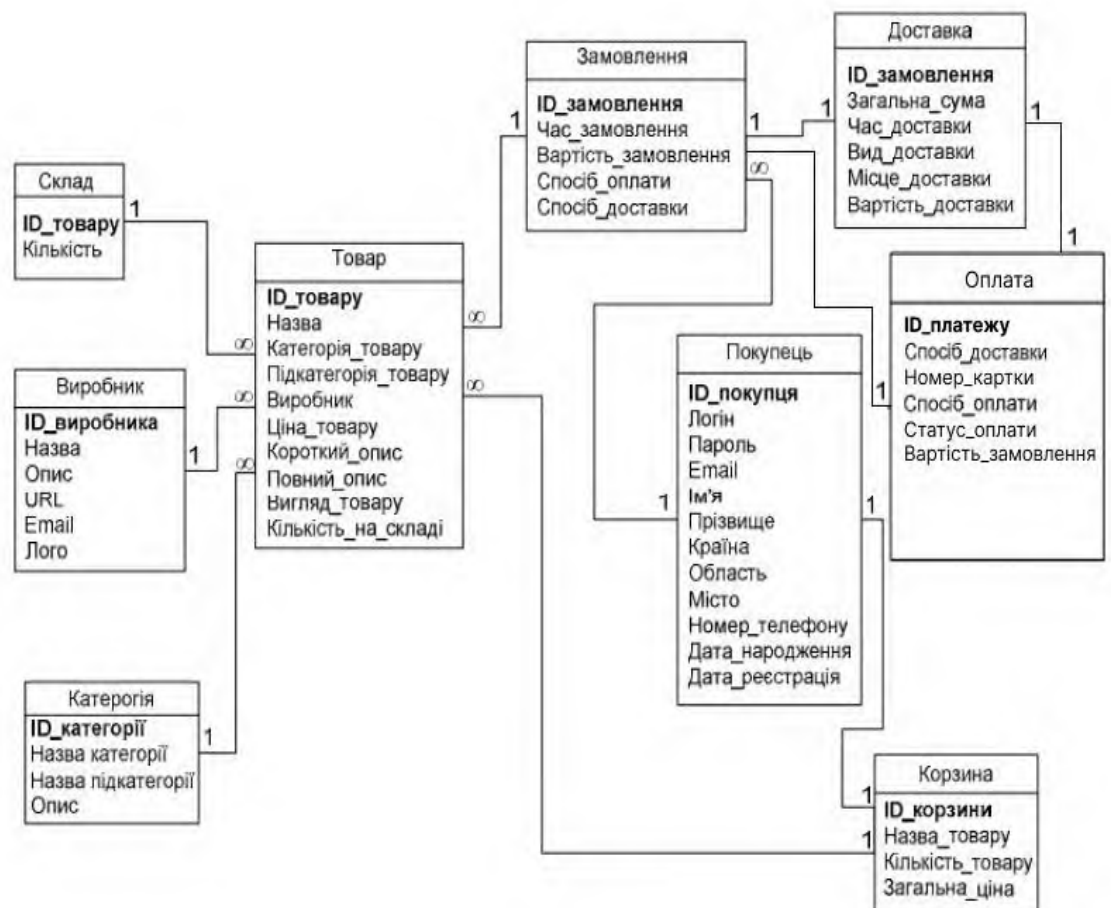


Рисунок 3.4 – Інформаційна модель бази даних електронного магазину.

Інформаційна модель електронного магазину визначає набір операцій, які виконуються. Основні функції можуть бути класифіковані за

категоріями, такими як управління користувачами, управління товарами, обробка замовлень та оплати.

- Функції для користувачів - елемент, що репрезентує особу, яка використовує систему;
- Товар - елемент, що відображає доступні для покупки продукти;
- Кошик - елемент, що представляє набір товарів, обраних користувачем для покупки;
- Замовлення - елемент, що представляє набір товарів, обраних користувачем для покупки;
- Оплата - елемент, що представляє набір товарів, обраних користувачем для покупки;
- Категорії - елемент, що представляє набір товарів, обраних користувачем для покупки.

3.2 Дослідження та аналіз оцінки критеріїв підвищення ефективності конкурентоспроможності електронного - магазину з урахуванням забезпечення інформаційної безпеки.

Для ефективного ведення бізнесу Інтернет-магазину необхідно провести дослідження та аналіз оцінки критеріїв підвищення ефективності його конкурентоспроможності. Тому, перед розробкою Інтернет-магазину як засобу підвищення ефективності конкурентоспроможності підприємства, були проаналізовані та досліджені деякі інші Інтернет-магазини, які входять в рейтинг найкращих, та які мають позитивні відгуки від користувачів. Для дослідження та аналізу були відібрані загальноприйняті критерії.

Критерій 1. Дотримання закону. Успішний інтернет-магазин дотримується правил торгівлі, встановленого законом.

Критерій 2. Юзабіліті сайту. У успішному інтернет-магазині сайт повинен бути максимально зручний для користування відвідувачами. Всі сторінки і посилання повинні бути видно і доступно.

Критерій 3. Інформаційні сторінки. В успішному інтернет-магазині повинні бути докладні інформаційні сторінки (необхідний мінімум):

- Про компанію (в тому числі історія);
- Оплата;
- Доставка;
- Гарантія;
- Контакти;
- Відгуки (реальні, а не вигадані);

Критерій 4. Вичерпна інформація про товар на сторінках товарів успішного інтернет-магазину завжди повинна бути наступна інформація:

- Наявність товару;
- Ціна товару;
- Детальний опис товару;
- Характеристики товару;
- Комплектація товару;
- Гарантія виробника та магазину на товар;

Критерій 5. Наявність всіх необхідні контактних даних. Успішний інтернет-магазин, завжди надає інформацію про себе:

- Всі телефони всіх служб;
- Час роботи офісу;
- Час роботи служби підтримки;
- Email;

Критерій 6. Замовлення зворотного дзвінка. В успішному інтернет-магазині завжди повинна працювати служба підтримки, яка може приймати замовлення на зворотний дзвінок від відвідувачів сайту.

Критерій 7. Онлайн-чат або наявність онлайн-консультанта. Оператори онлайн-чату в інтернет-магазині завжди повинні бути на місці, щоб будь-який відвідувач сайту зміг без праці зв'язатися з оператором і задати питання по цікавого товару її послуги інтернет-магазину.

Критерій 8. Способи оплати. Успішний інтернет-магазин повинен вміти приймати оплату всілякими способами. Чим більше способів оплати, тим краще. При цьому не повинно бути будь-яких додаткових комісій. Яка ціна товару вказана, таку і повинен платити покупець. Не більше.

Критерій 9. Акції та знижки Інтернет-магазин, зацікавлений в збільшенні продажів повинен постійно проводити акції і розпродажі, щоб стимулювати покупців до придбання товарів. А також заохочувати постійних покупців знижками і вигідними (для покупців і, природно, для інтернет-магазину) умовами на придбання інших товарів.

Критерій 10. Супровід замовлення Інтернет-магазин повинен супроводжувати замовлення в автоматичному і ручному режимі. Тобто повідомляти покупця про поточний статус замовлення за допомогою Email і по телефону (це мінімум, але достатній). До самого отримання замовлення покупцем.

Критерій 11. Додаткові опції для зручності клієнтів. Інтернет-магазин повинен пропонувати своїм відвідувачам зручні інструменти для користування сайтом і підбору товару. Це:

- Кошик товарів;
- Можливість резервування товару, якого немає в наявності;
- Можливість порівняння товарів;
- Швидкість оформлення замовлення;
- Категоризація асортименту;
- Фільтри відбору;
- Пошукова панель;
- Список бажань;
- Рейтинг товару;
- Відгуки, вибір можливостей та методів оплати.

Для дослідження та порівняння за вище наведеними критеріями обрані деякі Інтернет-магазини, які користуються популярністю.

Інтернет магазин «Розетка» - rozetka.ua. Останнім часом великої популярності і позитивні відгуки споживачів отримав онлайн-магазин «Розетка». Як розповідають його творці в розділі Про нас, їх робота на ІТ-ринку почалася ще в 1996 році, проте ера активного життя в Інтернеті стартувала в 2005 р. Фактично за два роки «Розетка» стала одним з лідерів мережевої торгівлі, а керівник цього проекту завоював почесну нагороду «Людина року» тижневика «Компьютерное Обозрение» за 2007 р в номінації «за найбільший внесок у розвиток ринку роздрібних продажів». Спочатку магазин позиціонував як продавець електроніки і є лідером в цьому сегменті, але зараз тут можна купити товари для дому, дачі, одяг для дорослих та дітей, алкоголь і навіть продукти. В асортименті Розетки понад 1,2 мільйона найменувань в різних категоріях. У плані дизайну і ергономіки сайт rozetka.ua слід визнати вельми вдалим. Асортимент магазину розбитий на три основні категорії: Комп'ютерні комплектуючі, Софт і Електроніка, в яких, в свою чергу, є підрозділи. У середині кожного з них діє сортування за ціною, параметрам, виробникам, що дозволяє потенційному покупцеві легко знайти потрібний йому товар. Незайвими нам здалися і рубрики Новини, Статті та огляди, де викладається корисна для споживача додаткова інформація. Доставка товару проводиться в усі регіони України. Електронний магазин, вдало побудований, інтуїтивно зрозумілий, внушає довіру, забезпечує комфортне перебування на ньому. Та є хорошим прикладом реалізації власного Інтернет магазину.

Також, досліджено Інтернет магазин Кэн, який спеціалізується на продажі комп'ютерної техніки та їх комплектуючих.

Інтернет магазин Кэн - <https://can.ua>. Так як і Інтернет магазин «Розетка» має каталог товарів, фільтри відбору, є позначки новинок та акційних товарів. Наведення на товар дає характеристику товару, але, в порівнянні з розеткою не одразу видно як його оцінують інші користувачі, необхідно більше кліків та переходів до необхідної інформації. Є електронна корзина, список бажань, порівняння товарів. Має інтуїтивно зрозумілий інтерфейс, має всі необхідні функції для пошуку та замовлення товарів.

Інтернет-магазин «ITCity» - <https://ITCity.com.ua>. Чимало позитивних відгуків на форумі і в коментарях до блогів викликав і магазин ITCity.com.ua. Споживачеві пропонується «джентльменський набір» товарів, що відносяться не тільки до сфер комп'ютерингу і персональних цифрових пристроїв, але також дрібна побутова і аудіо відеотехніка. Сайт магазину за своїм дизайном і функціональністю є зразком мінімалізму - нічого зайвого, тільки те, що потрібно для роботи користувача з ресурсом. Передбачено два варіанти покупки - традиційна для онлайн-магазинів Кошик і так званий Швидке замовлення з відправкою заповненої форми. Доставка проводиться як по Києву, так і по всій Україні (існує три варіанти для цього випадку).

Інтернет-магазин «Nout» - <https://nout.ua>. Пропонують техніку будь-яких напрямків - ноутбуки для дому, роботи, навчання і розваг, а також комп'ютери, планшети, неттопи і багато іншого. Вся техніка з каталогу реально є на складі, але також пропонується купити ноутбук і під замовлення, якщо не знайдено необхідної конкретної моделі. З огляду на різні фінансові можливості покупців, магазин ноутбуків Nout.ua об'єднав товари від бюджетного до преміум-класу, і за допомогою докладного фільтра пошуку є можливість підбирати.

Інтернет-магазин «Itbox» - <https://www.itbox.ua>. ITbox - Інтернет-магазин електроніки та комп'ютерної техніки. Комп'ютери, комплектуючі - широкий асортимент найкращих пропозицій, сезонні товари, святкові пропозиції, очікувані новинки, популярні бренди та категорії, статті та огляди, акції та знижки, підписка на новини. Інтернет-магазин має інтуїтивно зрозумілий інтерфейс. Потрапивши на головну сторінку можна звернутися до каталогу, в якому є можливість обирати необхідні категорії товарів. Після обраної категорії товару, для пошуку конкретного можна скористатися всілякими фільтрами відбору товарів та пошуковою панеллю. Не покидаючи сторінки видно характеристику товару. Є електронна корзина, список бажань, порівняння товарів.

Були досліджені Інтернет-магазини та проведено аналіз та порівняння згідно загальноприйнятих вище викладених критеріїв.

Результати порівняння Інтернет-магазинів представлені в таблиці 3.2.

Таблиця 3.2 - Оцінка Інтернет-магазинів за критеріями.

№	Критерії	Інтернет-магазини					Лідер
		Розетка	Кэн	ITCity	Nout	Itbox	
1	2	3	4	5	6	7	8
1	Дотримання закону	+	+	+	+	+	Розетка, Кэн, ITCity, Nout, Itbox
2	Юзабіліті сайту	+	+	+	+	+	Розетка, Кэн,ITCity, Nout, Itbox
3	Інформаційні сторінки: - Про компанію; - Оплата; - Доставка; - Гарантія; - Контакти; - Відгуки;	+	-	-	-	+	Розетка
		+	+	+	+	+	
		+	+	+	+	+	
		+	-	-	-	-	
		+	+	+	+	+	
		+	-	-	+	+	
4	Вичерпна інформація про товар на сторінках товарів: - Наявність товару; - Ціна товару; - Детальний опис товару; - Характеристики товару; - Комплектація товару; - Гарантія виробника та магазину на товар; - Рівень якості технологічного забезпечення - Документація та відповідність стандартам	+	+	+	+	+	Розетка
		+	+	+	+	+	
		+	+	+	+	+	
		+	+	+	+	+	
		+	-	-	+	-	
		+	-	-	-	-	

5	Наявність контактних даних: - Всі телефони всіх служб; - Час роботи офісу; - Час роботи служби підтримки; - Email;	+	+	+	+	+	Розетка
6	Замовлення зворотного дзвінка.	+	-	+	+	+	Розетка, ITCity, Nout, Itbox
7	Онлайн-чат або онлайн-консультант	+	-	-	-	+	Розетка, Itbox
8	Способи оплати	+	-	+	-	-	Розетка, ITCity
9	Акції та знижки Інтернет-магазину	+	+	+	+	+	Розетка, Кэн, ITCity, Nout, Itbox
10	Супровід замовлення Інтернет-магазину - Комунікація з клієнтами - Оптимізація пошуку та навігації по сайту - Програми лояльності та знижки	+	+	+	+	+	Розетка, Кэн, ITCity, Nout, Itbox
11	Додаткові опції для зручності клієнтів: - Кошик товарів; - Можливість резервування товару, якого немає в наявності; - Можливість порівняння товарів; - Швидкість оформлення замовлення; - Якість товарів та обслуговування - Підтримка різних мов та валют - Частота оновлення інформації на сайті - Якість зображень та	+	+	+	+	+	Розетка

	описів товарів - Оцінки та відгуки клієнтів						
	Категоризація асортименту: - Фільтри відбору; - Пошукова панель; - Список бажань; - Рейтинг товару; - Відгуки, вибір можливостей та методів оплати.	+	+	+	+	+	
		+	+	+	+	+	
		+	+	+	+	+	
		+	+	-	-	+	
		+	-	-	+	-	
		+	+	+	+	+	
	Забезпечення інформаційної безпеки: - Захист від DDoS-атак, - Швидкість завантаження сторінок, - Захист особистих даних, - Стабільність роботи сайту, - Політика безпеки та рівень обізнаності персоналу, - Безпека платежів, - Мобільна сумісність, - SEO оптимізація, - Загроза витоку особистої інформації через низький рівень захисту системи, - Загроза нових конкурентів.						
Результати		35	20	23	22	24	Розетка

Результати дослідження шляхом порівняння Інтернет-магазинів за критеріями показали, що всім критеріям задовольняє магазин «Розетка».

3.3 Визначення та оцінка впливу основних факторів конкурентоспроможності електронної комерції з урахуванням забезпечення інформаційної безпеки.

Як показали результати досліджень (існуючі онлайн-опитування, голосування, відгуки), найбільший пріоритет мають наступні фактори:

1. Зовнішній вигляд і зручність користування сайтом.

Сайт електронного магазину повинен бути зручним і зрозумілим користувачеві. Одним з доступних способів відстеження дій відвідувачів на сайті є технологія Вебвізор.

2. Коректно і «правильно» оформлений каталог товарів.

Інтуїтивно зрозуміла й логічна структура, широкий асортимент товарів привертають увагу покупців. Можливість швидко знайти потрібну відвідувачу категорію або конкретний товар збільшує шанси здійснення продажу.

3. Інформативна картка товару.

Сторінки з описом товару, найбільш значущі в Інтернет-магазині, яка повинна містити вичерпну інформацію для необхідності здійснення покупки: назва товару, правдивий опис, якісна ілюстрація, гарантії, опис умов доставки / оплати і повернення / обміну.

4. Інформація про доставку та оплату.

Покупцям важливо знати, як отримати і оплатити замовлений товар. Тому, необхідна перевірка, чи є в Інтернет-магазині відповіді на ці питання:

Можна забрати замовлення в офісі, чи доставляються тільки кур'єром?

О котрій годині відбувається доставка?

Які кур'єрські служби здійснюють доставку?

Яка вартість доставки?

Чи можна оплатити замовлення при отриманні, або потрібна передоплата?

Можна оплатити замовлення банківською картою або електронним платежем?

Необхідно надавати більше можливостей і кращі умови, щоб збільшити конверсію сайту.

5. Наявність гарантій.

Повинна вказуватися інформація про повернення товару та наявності гарантії. Адже при покупці в інтернет-магазині покупець боїться отримати бракований, неякісний або невідповідний йому товар. Необхідно повідомляти потенційному клієнтові, що магазин дотримується норм, встановлені Законом України «Про захист прав споживачів».

6. Комерційні показники сайту.

Наявність такої інформації, як прямий міський номер телефону в форматі 044-XXX-XX-XX або 0-800-XXX-XXX, є обов'язковим. Присутність тільки мобільних номерів недостатньо. Також обов'язкова наявність адреси офісу або пункту видачі, куди клієнт може приїхати. На сторінці «Контакти» повинна бути розміщена карта сайту. Рекомендовано розміщувати інтерактивну карту від пошукових систем, створену за допомогою спеціального конструктора.

7. Відгуки про товари і магазині.

Наявність позитивних відгуків як на самому сайті, так і на сторонніх ресурсах сприятливо позначається на ставленні до Інтернет-магазину і часто стає вирішальним фактором при прийнятті рішення про здійснення покупки. Якщо на сайті не передбачений функціонал розміщення відгуків, можна почати збирати відгуки на інших сайтах. Наприклад, створити тему на популярному міському або спеціалізованому форумі.

8. Аналіз статистики.

Проводиться порівняльний аналіз статистики схожих сайтів, якщо є відповідний доступ. До основних мінусів даного методу можна віднести недостатній обсяг даних і поверховість висновків.

9. Робота з відгуками відвідувачів.

На деяких сайтах спеціально для цього розміщують форми голосування та зворотного зв'язку. Для реалізації форми зворотного зв'язку на

сайті і обробити отримані відгуки необхідно періодично відстежувати думки відвідувачів. Мінус методу є те, що у відгуках будуть вказані тільки основні помилки, присутні на сайті.

10. *Тестування юзабіліті сайту інтернет магазину.*

Цей спосіб необхідний, якщо є сумніви в успіху нововведень на сайті. Для тестування сторінок можна використовувати спеціальний інструмент від Google - оптимізатор web-сайтів - і фокус-групи.

Використовуючи результати дослідження, проведемо експертну оцінку найбільш впливових факторів на ефективність конкурентоспроможності електронного - магазину з урахуванням забезпечення інформаційної безпеки.

Для визначення і оцінки ступеню впливу наведених факторів пропонується застосувати методи експертних оцінок та ймовірнісний підхід з використанням Байесовської мережі довіри (БМД).

На першому етапі дослідження проводилось визначення та експертиза найбільш впливових факторів для вирішення даної проблеми з використанням теорії експертних оцінок. Експертизу проводили експерти, які мають досвід у користуванні Інтернет мережею та сайтами, і по скільки необхідно визначити тільки ранги факторів, то погодженість їх оцінок доцільно визначати за допомогою множинного коефіцієнта конкордації K_0 запропонованого М. Кендаллом і Б. Смітом [19,20].

У якості експертів були залучені спеціалісти та користувачі Інтернет сторінок, де експертам (m) пропонувалося привласнити ранг (n) групам інформації перерахованих таблиці 3.3.

Погодженість думок експертів перевіряється за допомогою F - критерія Фішера [19,20]. Де через (X_{ij}) позначено ранг j -го виду інформації ($j = \overline{1, n}$) у ранжировці i -го експерта ($i = \overline{1, n}$). Для оцінки підготовленості експертів дотримуємось умови:

$$\sum_{j=1}^n X_{ij} = 0,5n(n + 1) \quad (3.5)$$

де: $\sum_{j=1}^n X_{ij}$ - сума рангів у ранжировці j -го експерта.

Погодженість експертів при ранжировці груп інформації оцінювалася коефіцієнтом конкордації (згоди):

$$K_0 = \frac{12S}{m^2(n^2-n)-m\sum_{i=1}^m T_i} \quad (3.6)$$

де: $S = \sum_{j=1}^n di^2$ - сума квадратів відхилень сум рангів, отриманих усіма групами інформації, від середньо – арифметичного сум рангів

$$d_j = X_j - 0,5m(n+1) \quad (3.7)$$

де: d - відхилення суми рангів j -го виду від середнього значення сум рангів по всім видам;

$$T_j = \sum_{\mu=1}^n (t_{\mu i}^3 - t_{\mu i}) \quad (3.8)$$

де: $T_{\mu i}$ - число повторень μ -го рангу в ранжировці i -го експерта.

При $K_0 = 1$ думка експертів вважається узгодженою повністю. При $K_0 < 1$, згідно з рекомендаціями для перевірки значимості погодженості визначаються значення статистики X^1 і X^2 :

$$X_{\text{набл}}^{(1)} = K_0 m(n-1) \quad (3.9)$$

$$X_{\text{набл}}^{(2)} = \frac{(m-1)X^{(1)}}{m(n-1)-X^{(1)}} \quad (3.10)$$

Після чого необхідно визначити числа ступенів свободи (ν_1) і (ν_2) розподілу, для чого обчислюються значення величин;

$$v_1 = n - 1, v_2 = \frac{L^2}{(m-1) \sum_{j=1}^n V_j^2} - (m - 1) \quad (3.11)$$

де: $L = (m - 1) \sum_{j=1}^n V_j$

$$V_j = \frac{1}{(m-1) \sum_{i=1}^m (X_{ij} - \bar{X}_j)^2} \quad (3.12)$$

$$\bar{X}_j = \frac{1}{m} \sum_{i=1}^m X_{ij}, \quad j = \overline{1, n}$$

По таблиці F – розподілу Фішера порівнюємо критичне значення $F_{кр.}$ при рівні значимості $\alpha = 0.05$ і числах ступеню свободи v_1 і v_2 . Порівнюючи отримане значення $X_{набл}$ зі значенням $F_{кр.}$ робимо висновок, що думки експертів можна вважати погодженими.

Результати експертного оцінювання наведені у таблиці 3.3.

Таблиця 3.3 – Результати експертного оцінювання впливових факторів конкурентоспроможності електронної комерції з урахуванням забезпечення інформаційної безпеки.

Експерти (m)	Фактори	Експертні оцінки (n)										Сума Σ
E1	Політика безпеки та рівень обізнаності персоналу	10	9	10	9	9	10	9	10	9	10	85
E2	Коректно і «правильно» оформлений каталог товарів.	9	8	8	9	8	8	9	8	8	9	80
E3	Безпека платежів	8	7	8	8	9	8	9	7	9	9	95
E4	Зовнішній вигляд і зручність користування сайтом.	9	8	7	9	8	7	8	8	7	9	92
E5	Інформативна картка товару .	6	7	7	6	7	8	9	7	8	9	74
E6	Інформація про доставку та оплату.	8	5	8	5	5	7	6	8	7	7	66
E7	Захист від DDoS-атак	10	8	9	9	8	10	8	10	9	10	82
E8	Якість товарів та обслуговування	6	8	7	8	7	9	8	9	6	9	77
E9	Наявність гарантій.	5	6	4	5	7	7	9	6	5	8	63

E10	Оптимізація пошуку та навігації по сайту	9	8	6	9	8	9	6	9	10	9	83
E11	Відгуки про товари в магазині.	10	7	8	10	10	9	10	9	10	9	80
E12	Оцінки та відгуки клієнтів	6	9	8	6	6	8	9	7	9	9	77
E13	Захист особистих даних	9	8	8	10	9	9	9	10	8	10	90
E14	Мобільна сумісність	8	8	6	9	7	9	8	7	9	9	80
E15	SEO оптимізація	9	9	7	9	7	7	8	6	8	9	79
E16	Комунікація з клієнтами	9	8	8	9	8	9	8	9	10	8	86
E17	Частота оновлення інформації на сайті	7	7	8	10	7	6	9	8	8	9	79
E18	Програми лояльності та знижки	6	4	6	8	9	5	8	7	9	6	68

За результатами експертного оцінювання (табл. 3.3) побудовані рангові діаграми розподілу по ступеню важливості факторів ефективності та безпеки електронної комерції (рис.3.3).

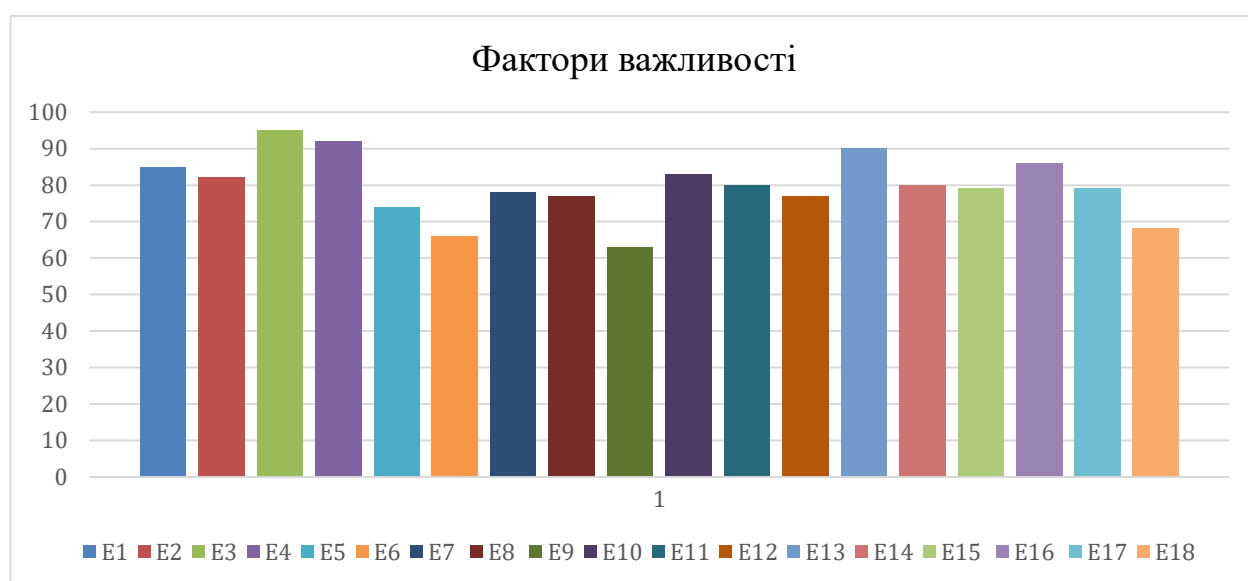


Рисунок 3.5 – Рангова діаграма розподілу ступеню важливості факторів.

3.4 Розробка та дослідження математичної моделі оцінки конкурентоспроможності електронної комерції з урахуванням забезпечення інформаційної безпеки.

На базі побудованої інформаційної моделі (п.3.1), та визначення основних впливових факторів ефективності електронної торгівлі (пп.3.2, 3.3) розробимо математичну модель оцінки конкурентоспроможності електронної

комерції з урахуванням забезпечення інформаційної безпеки на базі ймовірнісного методу з використанням Байєсовської мережі довіри (БМД).

Байєсівські мережі є потужним інструментом для моделювання ймовірнісних залежностей між змінними. Вони дозволяють оцінити вплив різних факторів на результативність системи, що є особливо корисним для аналізу складних систем, таких як інтернет-магазини. У даній роботі, мережа Байєса використовується для моделювання взаємодії між різними аспектами інтернет-магазину.

Байєсовська мережа довіри представляє собою графічні моделі, які ґрунтуються на принципах теорії ймовірностей та теорії графів. Вони складаються з пар $\langle G, V \rangle$, де G – це спрямований ациклічний граф, що представляє випадкові змінні, а V – набір параметрів, які визначають структуру системи.

Повна загальна ймовірність БМД обчислюється по формулі 3.13 [12]

$$P_B(X^{(1)}, \dots, X^{(N)}) = \prod_{i=1}^N P_B(X^{(i)} | P_A(X^{(i)})), \quad (3.13)$$

де A – множина станів модулів безпеки; $N = (x_1, \dots, x_N)$ – вектор параметрів їх розподілів.

Умовна ймовірність події визначається співвідношенням 3.14

$$p(E|H_k) = \frac{p(E \cap H_k)}{p(H_k)}, \quad (3.14)$$

де E й H_k – зв'язані між собою змінні. Ця залежність дозволяє визначити, яка буде ймовірність події E , якщо має місце конкретна подія H_k . Взаємовиключні події формують вичерпну множину у випадку зображеному формулою 3.15

$$\bigcup_{i=1}^n E_i = \Omega. \quad (3.15)$$

де $\sum P$ - сума значень імовірностей значення і-го фактору, при різних заданих значеннях вихідної змінної. Очевидно, що чим вище коефіцієнт максимальної зміни ймовірностей, тим більше чутлива система до даного вхідного параметра, отже, значимість даного параметра буде більш вагомою [34], [30].

На рис.3.6 побудована БМД оцінки ефективності електронної торгівлі.

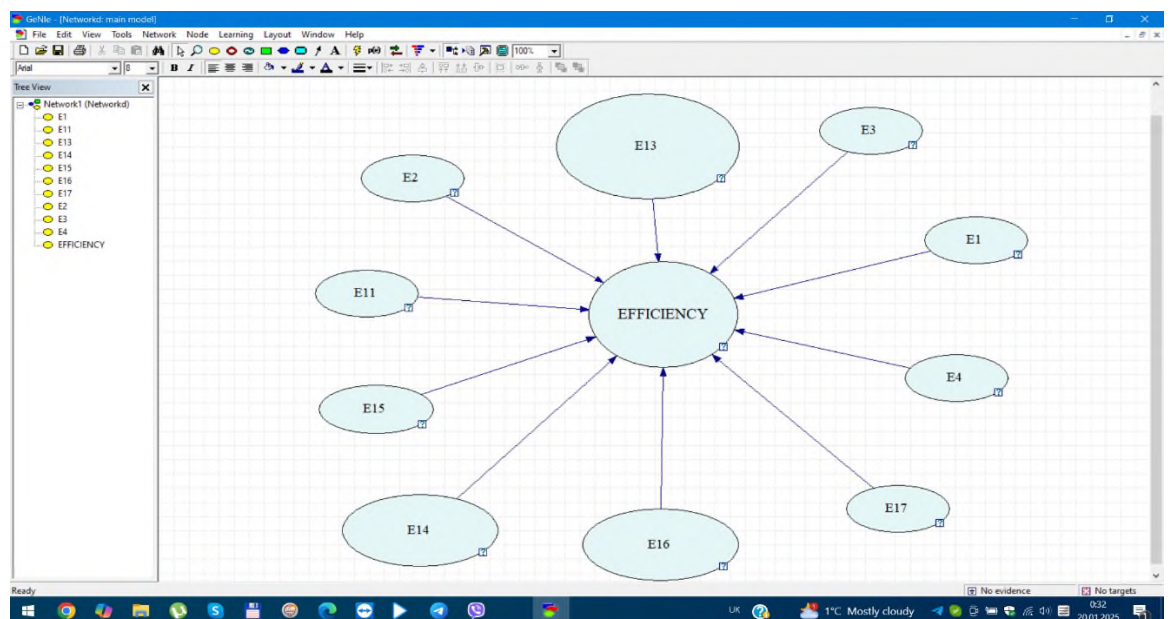


Рисунок 3.6 – Байесовська мережа довіри.

При побудові БМД, для заповнення вершин мережі, застосовувались знання та оцінки експертів. Результати експертних оцінок наведені в таблиці 3.2.

Таблиця 3.2 – Результати експертного оцінювання факторів.

Фактори впливу	E1	E2	E3	E4	E5	E6	E7	E8
Значний вплив	0,75-1	0,65-1	0,65-1	0,8-1	0,75-1	0,7-1	0,75-1	0,55-1
Незначний вплив	0-0,75	0-0,65	0-0,65	0-0,75	0-0,7	0-0,65	0-0,7	0-0,5

Фактори впливу	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18
Значний вплив	0,7-1	0,7-1	0,55-1	0,65-1	0,7-1	0,75-1	0,75-1	0,6-1	0,5-1	0,35-1
Незначний вплив	0-0,65	0-0,65	0-0,5	0-0,6	0-0,65	0-0,7	0-0,7	0-0,55	0-0,45	0-0,3

3.4.1 Формування граф-теоретичної моделі Байесовської мережі довіри та оцінка впливу основних факторів безпеки на ефективність роботи електронної комерції.

Для моделювання було використано програмне забезпечення GeNIe 2.0, яке дозволяє будувати та аналізувати Байєсівські мережі. Вузли мережі представляють фактори, що впливають на ефективність роботи інтернет-магазину, такі як захист від DDoS атак, захист даних та стабільність роботи сайту.

Визначення вузлів та зв'язків.

Вузли: Кожен вузол представляє окремий фактор, що впливає на ефективність. Наприклад, вузли E1, E2 та E4 відповідають за захист від DDoS атак, захист даних та стабільність роботи сайту відповідно.

Зв'язки: Стрілки між вузлами показують причинно-наслідкові залежності. Вихідні значення кожного вузла впливають на ймовірності результативних вузлів, зокрема, на ефективність (Efficiency).

Побудова графу:

Граф будується шляхом додавання вузлів та встановлення зв'язків між ними відповідно до причинно-наслідкових залежностей. Наприклад, вузли E1, E2 та E4 мають прямий вплив на вузол Efficiency.

Встановлення ймовірностей (CPT):

Для кожного вузла визначається таблиця умовних ймовірностей (CPT), яка показує ймовірність кожного стану вузла в залежності від станів

вузлів-предків. Наприклад, ймовірності для вузла Efficiency залежать від станів вузлів E1, E2 та E4.

Аналіз результатів:

Низька оцінка стану ефективності інтернет-магазину:

Мережа 1 (Рисунок 3.7):

Ефективність: 50% (ефективність), 50% (неефективність)

Вузли: E1 (high - 0%, average - 100%, low - 0%), E2 (high - 0%, average - 100%, low - 0%), E4 (high - 0%, average - 100%, low - 0%)

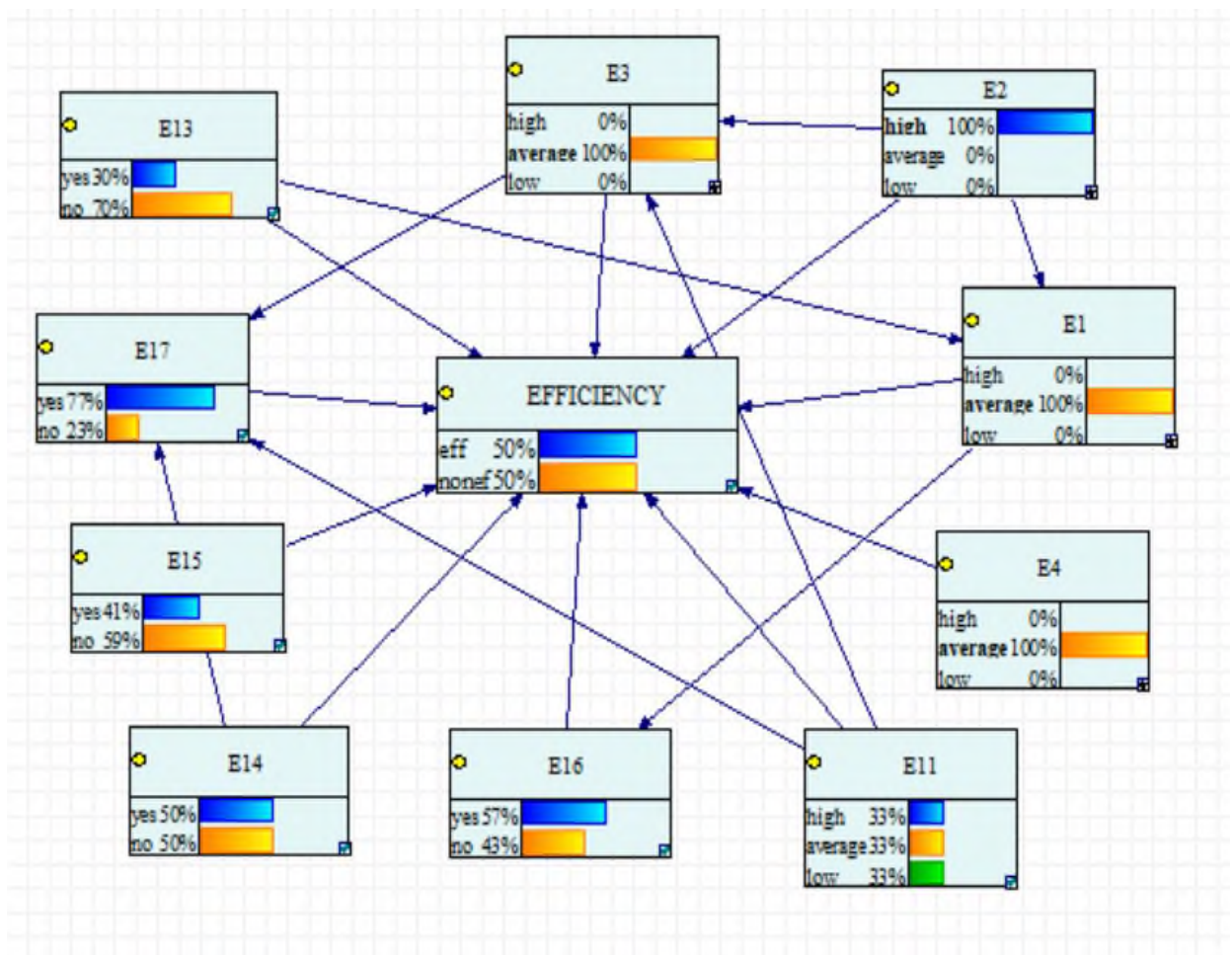


Рисунок 3.7 – Низька оцінка стану ефективності інтернет-магазину.

Середня оцінка стану ефективності інтернет-магазину:

Мережа 2 (Рисунок 3.8):

Ефективність: 77% (ефективність), 23% (неефективність)

Вузли: E1 (high - 0%, average - 0%, low - 100%), E2 (high - 0%, average - 0%, low - 100%), E4 (high - 0%, average - 0%, low - 100%)

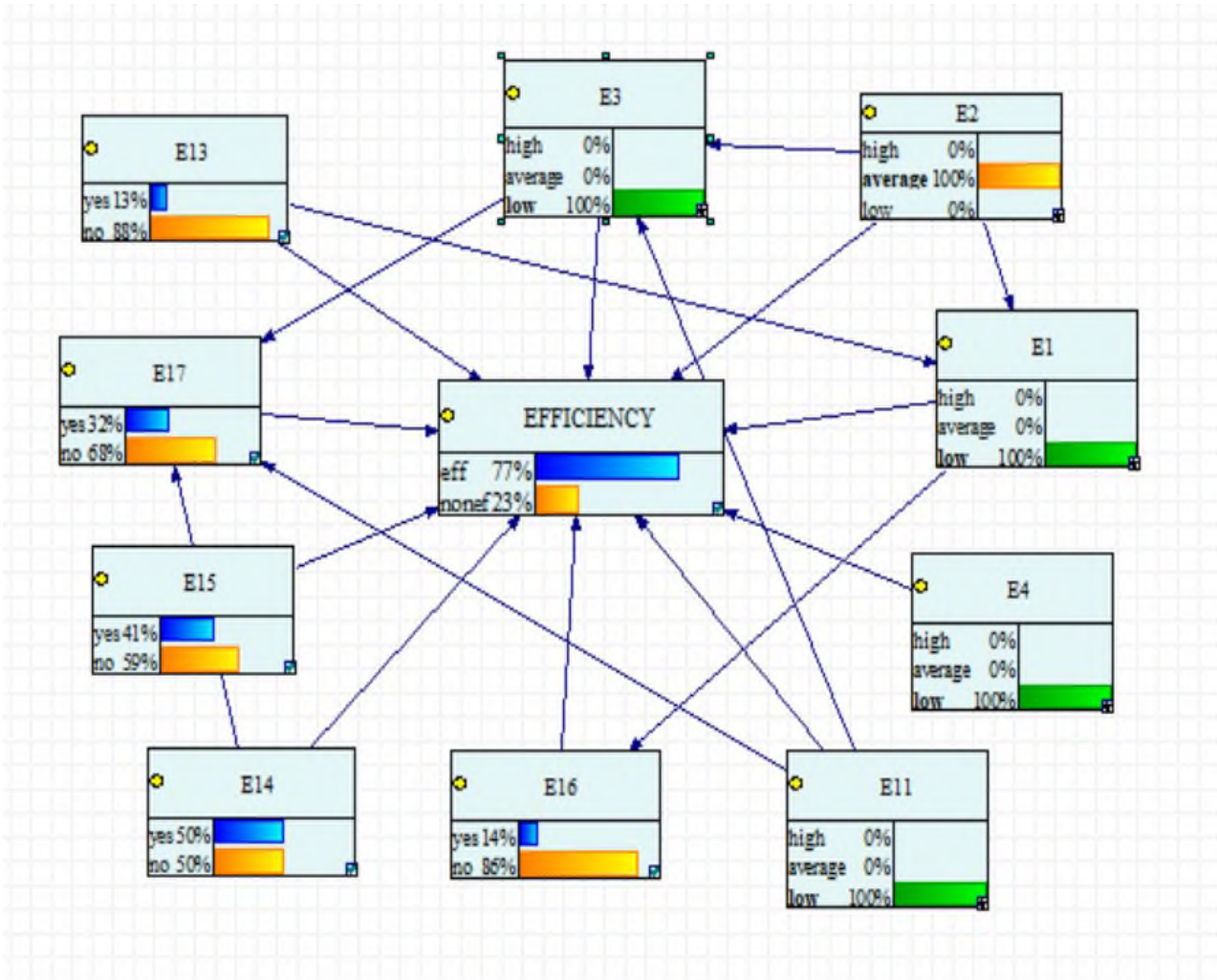


Рисунок 3.8 – Середня оцінка стану ефективності інтернет-магазину.

Висока оцінка стану ефективності інтернет-магазину:

Мережа 3 (Рисунок 3.9):

Ефективність: 88% (ефективність), 12% (неефективність)

Вузли: E1 (high - 26%, average - 28%, low - 46%), E2 (high - 33%, average - 36%, low - 31%), E4 (high - 30%, average - 30%, low - 40%)

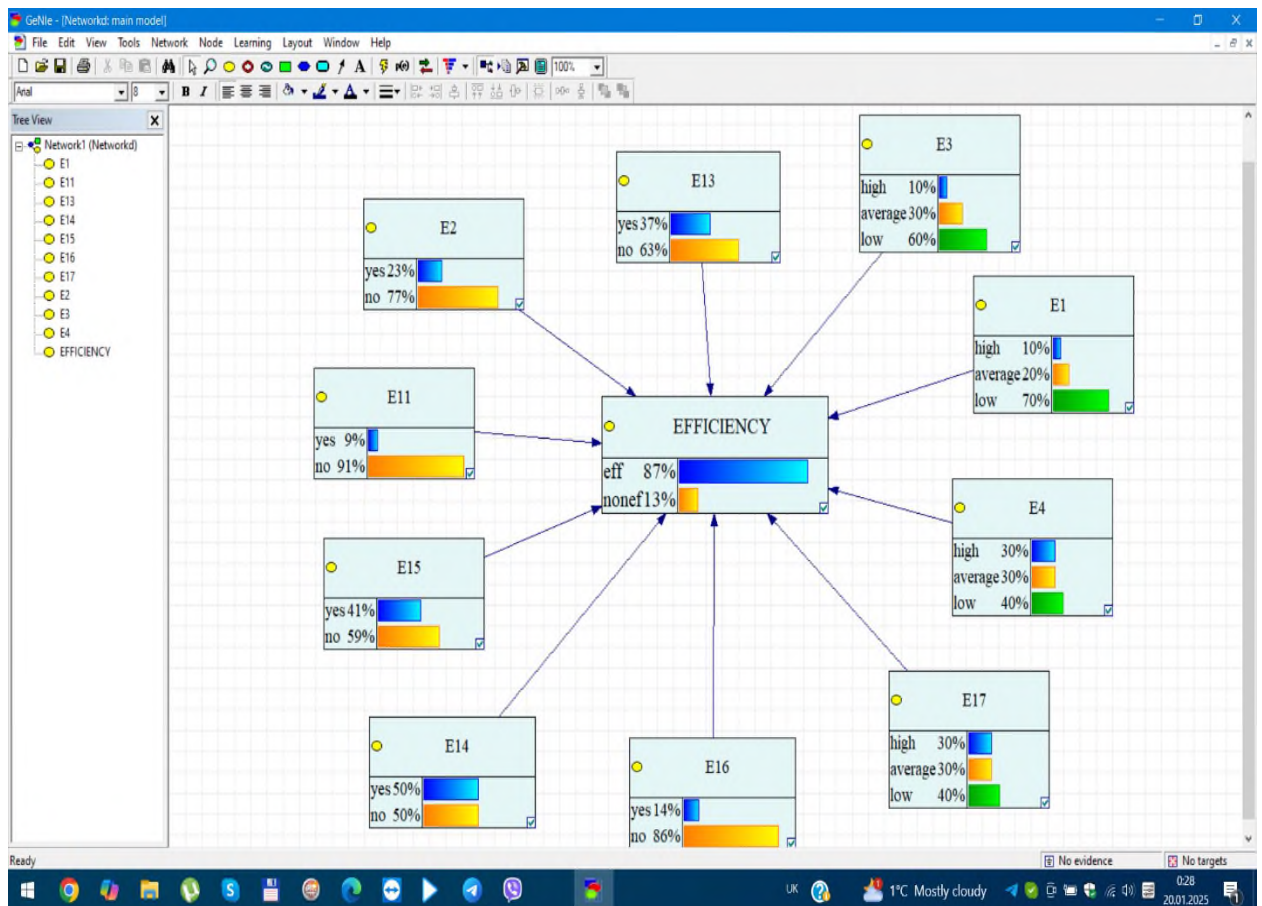


Рисунок 3.9 – Висока оцінка стану ефективності інтернет-магазину.

За результатами моделювання видно, що початковий стан мережі показав, що ймовірність ефективності становила лише 50%, що свідчить про те, що без належних заходів безпеки інтернет-магазин не здатен працювати на високому рівні ефективності.

Вузол E7 (Захист від DDoS атак): При збільшенні рівня захисту до високого рівня, ймовірність ефективності зросла до 77%. Це показує, що покращення захисту від DDoS атак є критичним для загального підвищення ефективності.

Вузол E13 (Захист даних клієнтів): Покращення захисту даних клієнтів також значно вплинуло на ефективність. Висока ймовірність захисту даних призвела до зростання ефективності до 88%.

Вузол E1 (Політика безпеки та рівень обізнаності персоналу): також позитивно впливає на ефективність інтернет-магазину.

Встановлення високих рівнів безпеки у вузлах E1, E7 та E13 дозволило досягти ймовірності ефективності на рівні 88%, що значно перевищує початковий показник у 50%. Це підтверджує важливість інвестування в безпеку для забезпечення стабільної та ефективної роботи інтернет-магазину.

Рекомендації для інтернет-магазинів:

1. Захист від DDoS атак (E7): Забезпечити високий рівень захисту від DDoS атак для всіх компонентів системи.
2. Захист даних клієнтів (E13): Впровадити сучасні технології для захисту персональних даних клієнтів.
3. Стабільність роботи сайту E1 (Політика безпеки та рівень обізнаності персоналу): Забезпечити безперебійну роботу сайту шляхом регулярного моніторингу та підтримки.

На основі проведеного аналізу можна зробити висновок, що покращення рівня безпеки є ключовим фактором для досягнення загального підвищення ефективності роботи інтернет-магазину. Зокрема, заходи щодо підвищення захисту від DDoS атак, захисту даних клієнтів та забезпечення стабільності роботи інтернет магазину мають значний позитивний вплив на ефективність.

Виконання цих рекомендацій допоможе інтернет-магазинам підвищити свою ефективність і забезпечити стійке зростання в умовах сучасних викликів інформаційної та кібернетичної безпеки.

Висновки до четвертого розділу. У даному розділі для побудови та дослідження інформаційної і математичної моделей ефективності роботи електронного магазину з урахуванням забезпечення інформаційної безпеки, застосовані теоретичні та практичні методи застосування теорії м'яких обчислень, системний аналіз, графо-аналітичні методи Байесовської мережі довіри та теорія експертних оцінок.

Для підвищення ефективності роботи інтернет – магазину проведено дослідження інформаційних потоків та розроблена інформаційна модель інтернет торгівлі.

У розділі також проведено дослідження та аналіз критеріїв підвищення ефективності конкурентоспроможності електронного - магазину з урахуванням забезпечення інформаційної безпеки. Розроблено та досліджено математичну модель оцінки впливу основних факторів конкурентоспроможності електронної комерції з урахуванням забезпечення інформаційної безпеки.

На основі проведеного аналізу визначені та запропоновані рекомендації, які допоможуть інтернет-магазинам підвищити свою ефективність і забезпечити стійке зростання в умовах сучасних викликів інформаційної та кібернетичної безпеки.

4. ПРАКТИЧНА РЕАЛІЗАЦІЯ

4.1 Вибір методу шифрування в системі онлайн магазину.

Шифрування і пов'язані з ним технології широко і часто використовуються як засіб забезпечення безпеки інформації, а його важливість все зростає при більшому використанні Інтернету. Історія шифрування – це історія «конкурсу дотепності» між розробниками шифрування і шифрувальними кодами. Кожен раз, коли створюється новий алгоритм шифрування, він розшифровується і, у свою чергу, призводить до створення нового алгоритму шифрування, а цикли створення і дешифрування алгоритмів повторюються і до цього дня.

Класичні шифри (стародавні часи) – ієрогліфи (піктограми, які використовуються в Стародавньому Єгипті), записані на стелі приблизно в 3000 році до нашої ери, вважаються найстарішим збереженим прикладом шифрування. Ієрогліфи довго вважалися неможливими для читання, але відкриття і вивчення Розівського каменю в XIX столітті було каталізатором, який дозволив читати ієрогліфи.

Методи шифрування, такі як «scytale cipher», які покладаються на перестановку послідовності, в якій зчитуються символи, називаються «шифрами транспонування». Непарний шифр, що з'явився в I столітті до нашої ери, був названий так тому, що він часто використовувався Юлієм Цезарем, і це особливо відомий метод шифрування серед безлічі методів, що виникли протягом довгої історії шифрування. Метод Цезаря включає заміну кожної букви алфавіту в початковому тексті буквою, розташованою на багатьох місцях, розташованих далі по послідовності букв в алфавіті. Відправник і одержувач заздалегідь погоджуються замінити кожну літеру тексту буквою, яка, наприклад, зміщена на три позиції в алфавіті. На даний час існує також багато видів шифрування, які є уже сучасними та застосовуються під час шифрування інформації, яка зберігається на електронних носіях. Є два основних види шифрування інформації – симетричне та асиметричне.

Симетричне шифрування – це один із видів шифрування, в якому для шифрування і дешифрування застосовується один і той же самий ключ. Такий метод набрав популярності в останні десятиліття, для полегшення спілкування уряду і військових. У даний час симетричні ключі широко використовуються в різних типах комп'ютерних систем для захисту особистих даних. Симетрична схема шифрування заснована на одному ключі, який використовується двома або більше користувачами. Цей же ключ використовується для шифрування і дешифрування так званого відкритого тексту (який містить повідомлення або частину закодованих даних). Процес шифрування складається з обробки відкритого тексту алгоритмом шифрування, так званим шифром, який у свою чергу генерує зашифрований текст. Якщо схема шифрування достатньо надійна, єдиний спосіб для людини прочитати або отримати доступ до інформації, що міститься в зашифрованому тексті, це використати відповідний ключ для його розшифрування. Процес розшифрування в основному перетворює зашифрований текст назад у відкритий [51].

Асиметричне шифрування – це система шифрування, яка використовує як відкритий, так і закритий ключі, на відміну від єдиного ключа, який застосовується у симетричній системі. Використання пар ключів дає унікальний набір характеристик і можливостей, які можна використовувати для розв'язання проблем, властивих іншим криптографічним методам. Ця форма криптографії стала важливим елементом сучасної комп'ютерної безпеки [52].

Симетричні та асиметричні системи шифрування широко використовують в усьому світі, на багатьох сучасних підприємствах та у багатьох компаніях. Застосування алгоритмів асиметричної криптографії – це аутентифікація даних з використанням цифрових підписів. По суті, цифровий підпис – це хеш, створений з використанням даних у повідомленні. Коли це повідомлення відправлено, одержувач може перевірити підпис, використовуючи відкритий ключ відправника, щоб перевірити справжність джерела повідомлення і переконатися, що воно не було підроблено. У деяких випадках цифрові підписи та шифрування застосовуються разом, бо сам хеш може бути зашифрований як

частина повідомлення. Слід зазначити, що не всі схеми цифрового підпису використовують метод шифрування. Асиметричний тип шифрування використовується багатьма сучасними комп'ютерними системами для забезпечення безпеки конфіденційної інформації. Наприклад, електронні листи можуть бути зашифровані з використанням методів криптографії з відкритим ключем для забезпечення конфіденційності їх вмісту. Протокол рівня захищених сокетів (SSL), який робить можливим безпечне підключення до веб-сайтів, також використовує асиметричну криптографію. Системи РКС навіть використовувалися для забезпечення безпечного середовища електронного голосування, яка потенційно дозволяла б виборцям брати участь у виборах зі своїх домашніх комп'ютерів.

Симетричні алгоритми шифрування використовуються в багатьох сучасних комп'ютерних системах для підвищення безпеки даних і конфіденційності користувачів. Розширений стандарт шифрування (AES), який широко використовується як в додатках для безпечного обміну повідомленнями, так і в хмарних сховищах, є одним з яскравих прикладів симетричного шифру та перспективи його застосування в подальшому.

4.2 Алгоритм роботи методу шифрування RSA.

В основі методу шифрування RSA лежить використання двох ключів: відкритого ключа для шифрування та закритого ключа для дешифрування. Цей підхід забезпечує безпечний обмін відкритими ключами без розкриття закритого ключа, який залишається виключно у власності власника ключа. RSA використовується не лише для шифрування, але й для цифрових підписів, що забезпечує автентифікацію повідомлень. Його безпека базується на проблемі розкладання великих простих чисел, що ускладнює його. Даний метод широко використовується для захисту електронної пошти, встановлення безпечних з'єднань у веб-браузерах, цифрового підпису документів та різноманітних інших програм, а також RSA є також важливим інструментом для забезпечення безпеки в електронному магазині для

забезпечення: Аутентифікація користувачів, Захисту транзакцій, Обмін ключами.

У шифруванні методом RSA використовується асиметричний алгоритм шифрування, що базується на математичних властивостях чисел і основах теорії чисел. Основні математичні аспекти RSA включають:

Великі прості числа. Основою RSA є вибір двох великих простих чисел, позначених як p та q . Ці числа служать основою для обчислення модулю n , який визначається як $n = p * q$. Величина числа n відіграє ключову роль у процесі шифрування та дешифрування.

Ейлерова функція. Для обчислення приватного ключа використовується ейлерова функція $\phi(n)$, де n - це модуль, а ϕ - ейлерова функція. Для простого числа p , $\phi(p) = p - 1$. Однак для модулю $n = p * q$, $\phi(n) = (p - 1) * (q - 1)$

Відкритий і приватний ключі. Відкритий ключ складається з модуля n та публічного експонента e , де e є відкритим експонентом. Приватний ключ включає модуль n та приватний експонент d , де d є приватним експонентом. Вони обчислюються так, щоб виконувалася рівність $e * d \equiv 1(mod \phi(n))$, що визначає взаємно простість e та $\phi(n)$.

Шифрування та Дешифрування. Процес шифрування в RSA використовується з відкритим ключем та включає підняття повідомлення m до ступеня e у модулі n , тобто $c \equiv m^e(mod n)$, де c - шифротекст.

Процес дешифрування використовується з приватним ключем та включає підняття шифротексту c до ступеня d у модулі n , тобто $m \equiv c^d(mod n)$, де m - відновлене повідомлення.

Безпека RSA ґрунтується на складності завдання факторизації великих простих чисел. Для ефективного факторизації n потрібно розкласти його на прості множники p та q . У зв'язку з величезними розмірами великих чисел, таке завдання є складним.

Алгоритм роботи RSA є асиметричним, тобто кожен користувач має свою особисту та унікальну пару ключів(приватний та публічний). Приватний

ключ тримається засекреченим. Тільки користувач знає свій приватний ключ, при цьому публічний ключ може бути навіть завантажений в інтернет(бути відомим всім). Єдиний спосіб розшифрувати повідомлення, яке було зашифроване відкритим ключем, це використати приватний ключ.

Алгоритм RSA складається з чотирьох етапів: 1) генерація ключа; 2) розподіл ключа; 3) шифрування; 4) дешифрування.

4.3 Застосування методу шифрування RSA у системах електронної комерції.

Аутентифікація користувачів. Одним з основних застосувань алгоритму RSA є створення цифрових підписів. Цифровий підпис – це електронна “печатка”, яка підтверджує автентичність та цілісність документа або повідомлення. Використовуючи алгоритм RSA, можна забезпечити, що підписаний документ не був змінений та що тільки власник відповідного приватного ключа міг здійснити підпис.

При реєстрації нового користувача в системі йому генерується унікальна пара ключів - публічний та приватний. Публічний ключ розголошується та зберігається в базі даних системи, тоді як приватний ключ залишається тільки у власника.

Алгоритм RSA в класичній реалізації для шифрування інформації та створення цифрових підписів виглядає таким чином: Допустимо, що Користувач1 (K1) хоче відправити Користувачу2 (K2) повідомлення M. K1 створює зашифрований текст C, взводячи повідомлення M в ступінь e і множачи на модуль n:

$$C = M^e(mod\ n) \quad (4.6)$$

де e і n є відкритим ключем K2. K1 потім посилає C (зашифрований текст) для K2. Для того, щоб розшифрувати отриманий текст, K2 піднесе отриманий зашифрований текст C до степеню d і помножить його на модуль n:

$$M = C^d(mod\ n) \quad (4.7)$$

зв'язок між e та d гарантує, що K_2 точно обрахує M . Так як тільки K_2 знає d , то тільки він має тільки можливість розшифрувати отримане повідомлення.

Розглянутий алгоритм підтверджує, що власник і тільки власник секретного ключа d може створити ЕЦП для деякого документу M , а визначити секретний ключ d по відкритому ключу e не простіше, ніж вирішити задачу факторизації модуля $n = p * q$.

Окрім цього, можливо продемонструвати математично, що результати перевірки ЕЦП буде позитивним тільки в тому випадку, якщо таємний ключ d , що відповідає публічному ключу e , використовується в шифруванні ЕЦП. Виходячи з цього, відкритий ключ e можна назвати ідентифікатором відправника.

Для забезпечення криптографічної стійкості підпису RSA, необхідно використовувати цілі числа d , e . і n не менше, ніж 2^{512} (близько 10^{154}).

4.3.1 Робота протоколів SSL/TLS із використання алгоритму RSA.

Метод RSA є ключовою складовою протоколів SSL та TLS, які використовуються для захисту з'єднань між веб-сайтами та браузерами користувачів. Це забезпечує безпечне середовище для електронної комерції, де користувачі можуть відчувати себе впевнено, роблячи покупки онлайн [40].

Протоколи SSL (Secure Sockets Layer) та TLS (Transport Layer Security) забезпечують безпеку з'єднань між веб-сайтами та браузерами користувачів [41].

1. Початковий етап (Handshake): Під час SSL/TLS handshake, сервер надсилає свій цифровий сертифікат, який містить відкритий ключ RSA, до клієнта. Клієнт використовує цей відкритий ключ для шифрування випадково згенерованого сеансового ключа, який потім надсилається назад на сервер [42].

2. Шифрування даних: Сервер використовує свій приватний ключ RSA для розшифрування сеансового ключа, отриманого від клієнта. Цей сеансовий ключ потім використовується для шифрування подальшого обміну даними між клієнтом та сервером.

3. Забезпечення цілісності: RSA також використовується для створення цифрових підписів, які допомагають забезпечити цілісність та автентичність переданих даних. Цифровий підпис гарантує, що дані не були змінені під час передачі.

4. Завершення з'єднання: Після завершення сеансу, сеансовий ключ видаляється, що забезпечує, що кожна сесія має унікальний ключ і не може бути використана повторно.

Використання RSA в SSL/TLS дозволяє забезпечити безпечний обмін ключами та захистити дані від несанкціонованого доступу, забезпечуючи конфіденційність та цілісність інформації, що передається через Інтернет.

Розробка програмного коду із застосуванням методу шифрування RSA в системі онлайн магазину реалізована на мові програмування Python:

```
import random
import math
```

```
# n= p.q
```

```
#phi(n) = phi(p.q)=phi(p).phi(q) = (p-1). (q-1)
```

```
#phi(n) = (p-1.q-1)
```

```
def is_prime (number):
```

```
    if number < 2:
```

```
        return False
```

```
    for i in range (2, number // 2 +1):
```

```
        if number % i == 0:
```

```
            return False
```

```
    return True
```

```
def generate_prime (min_value, max_value):
```

```
    prime = random.randint (min_value, max_value)
```

```
    while not is_prime(prime):
```

```
        prime = random.randint(min_value, max_value)
```

```

return prime

def mod_inverse(e, phi):
    for d in range (3, phi):
        if (d * e) % phi == 1:
            return d
    raise ValueError ("Mod_inverse does not exist!")

p, q = generate_prime(1000, 50000), generate_prime ( 1000, 50000)
while p==q:
    q= generate_prime(1000, 50000)

n = p * q
phi_n = (p-1) * (q-1)

e = random.randint (3, phi_n-1)
while math.gcd(e, phi_n) != 1: #gcd=greater common denominator    != not equal
    e = random.randint (3, phi_n - 1)

d = mod_inverse(e, phi_n)

message = input("Enter your message to Encrypt ")

print ("Prime number P: ", p)
print ("Prime number q: ", q)
print ("Public Key: ", e)
print ("Private Key: ", d)
print ("n: ", n)
print ("Phi of n: ", phi_n, " Secret")

```

```

message_encoded = [ord(ch) for ch in message]

print ("Message in ASCII code: ", message_encoded)

# (m ^ e) mod n = c
ciphertext = [pow(ch, e, n) for ch in message_encoded]

print (message," Ciphared in: ", ciphertext)

Decodemsg= [pow(ch, d, n) for ch in ciphertext]
print ("back to ASCII: ", Decodemsg)
msg = "".join (chr(ch) for ch in Decodemsg)
print("from ASCII to TEXT: ", msg)

```

Коментар програми:

1. ``import random``: Імпорт бібліотеки ``random``, яка використовується для генерації випадкових чисел.
2. ``import math``: Імпорт модуля ``math``, який містить математичні функції, такі як ``gcd`` (найбільший спільний дільник).
3. ``is_prime(number)``: Функція, яка перевіряє, чи є задане число простим.
4. ``generate_prime(min_value, max_value)``: Функція, яка генерує випадкове просте число у заданому діапазоні.
5. ``mod_inverse(e, phi)``: Функція, яка знаходить мультиплікативно обернене за модулем ``phi``.
6. Генерування двох випадкових простих чисел ``p`` та ``q``, і визначення ``n``, яке дорівнює їхньому добутку.
7. Визначення ``phi_n``, яке дорівнює ``(p-1)*(q-1)``.
8. Вибір публічного ключа ``e`` (відкритий ключ) так, щоб він був взаємно простий з ``phi_n``.

9. Обчислення приватного ключа d , який є мультиплікативним оберненим для e за модулем ϕ_n .

10. Введення користувачем повідомлення для шифрування.

11. Шифрування повідомлення: перетворення кожного символу повідомлення в ASCII код і застосування формули $(m^e) \bmod n$, де m - ASCII код символу, e - публічний ключ і n - модуль.

12. Декодування зашифрованого повідомлення: застосування формули $(c^d) \bmod n$, де c - шифротекст, d - приватний ключ і n - модуль.

13. Виведення результатів.

Застосування даного коду в інтернет-магазині дає можливість забезпечити безпеку та конфіденційність інформації для шифрування особистих даних користувачів, таких як електронні адреси, паролі, номери платіжних карт та інші конфіденційні дані, які вони вводять під час реєстрації або оформлення замовлення, що дозволить забезпечити захист даних від несанкціонованого доступу та зловмисних атак.

Висновки до четвертого розділу. У даному розділі проведено аналіз та вибір методу шифрування в системі онлайн магазину. Детально проаналізовані симетричні та асиметричні алгоритми шифрування, які використовуються в багатьох сучасних системах для підвищення безпеки даних і конфіденційності користувачів. Розглянуто стандарти шифрування, які широко використовується як в додатках для безпечного обміну повідомленнями, так і в хмарних сховищах, та перспективи їх застосування в подальшому.

Запропонований алгоритм роботи методу шифрування RSA, який забезпечує безпечний обмін відкритими ключами без розкриття закритого ключа, та залишається виключно у власності власника ключа. RSA використовується не лише для шифрування, але й для цифрових підписів, що забезпечує автентифікацію повідомлень.

Розроблено програмний код із застосуванням методу шифрування RSA в системі онлайн магазину на мові програмування Python. Застосування даного коду в інтернет-магазині дає можливість забезпечити безпеку та конфіденційність інформації для шифрування особистих даних користувачів, таких як електронні адреси, паролі, номери платіжних карт та інші конфіденційні дані, які вони вводять під час реєстрації або оформлення замовлення, що дозволить забезпечити захист даних від несанкціонованого доступу та зловмисних атак.

ВИСНОВКИ

У роботі досліджена проблема створення та аналізу стратегії електронної комерції. Проведено детальний аналіз основних проблем, пов'язаних із захищеністю інтернет-магазину, визначено ключові фактори впливу загроз на електронну комерцію. Зосереджено увагу на детальному аналізі сучасних методів та засобів для оцінки та підтримки захищеності інформаційних ресурсів електронних магазинів.

Проведено дослідження інформаційних потоків роботи інтернет магазину, та побудована Інформаційна та інформаційно-логічна моделі з урахуванням забезпечення інформаційної безпеки. Для забезпечення безпеки роботи інтернет магазину застосовано метод шифрування RSA.

Для дослідження і визначення впливових факторів конкурентоспроможності та оцінки рівня захищеності електронної торгівлі використані системний аналіз, графо-аналітичні методи Байєсівської мережі довіри та теорія експертних оцінок.

Байєсовська мережа довіри, яка використана для оцінки роботи інтернет-магазину, продемонструвала необхідність вдосконалення захисних заходів. Після впровадження первинних заходів безпеки (Мережа 2) ймовірність ефективності зросла до 77%. Завдяки поліпшенню рівня захисту від DDoS-атак (E1), захисту інформації клієнтів (E2) та стабілізації роботи сайту (E4) (Мережа 3) ефективність досягла 88%.

Використання теоретичних та практичних підходів допоможе вирішити завдання з оцінки підвищення ефективності і безпеки електронного магазину, зокрема при урахуванні їхнього рівня невизначеності та суб'єктивності.

1. Доктрина інформаційної безпеки України від 25 лютого 2017 року №47/2017
2. Закон «Про критичну інфраструктуру» від 16.11.2021 Форма доступу - <https://zakon.rada.gov.ua/laws/show/1882-20>
3. Закон України Про національну безпеку України Форма доступу - <https://zakon.rada.gov.ua/laws/show/2469-VIII>
4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" Указ Президента України; Стратегія від 26.08.2021 Форма доступу - <https://www.president.gov.ua/documents/4472021-40013>
5. Закон України Про основні засади забезпечення КБ Форма доступу - <https://zakon.rada.gov.ua/laws/show/2163-19>
6. Закон України «Про інформацію» Редакція від 16.07.2020 Форма доступу - <https://zakon.rada.gov.ua/laws/show/2657-12>
7. Закон України «Про захист інформації в інформаційно телекомунікаційних системах» Редакція від 04.07.2020 Форма доступу - <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
8. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» Редакція від 10.02.2021 Форма доступу - <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF>
9. Закон України «Про захист персональних даних» Редакція від 15.12.2021 Форма доступу - <https://zakon.rada.gov.ua/laws/show/2297-17>
10. Закон України «Про державну таємницю» Редакція від 24.11.2021 Форма доступу - <https://zakon.rada.gov.ua/laws/show/3855-12>
10. ЕЛЕКТРОННА КОМЕРЦІЯ В УМОВАХ КОНКУРЕНЦІЇ, ЯК СУЧАСНА ФОРМА ОРГАНІЗАЦІЇ БІЗНЕСУ - URL: <http://dspace.idgu.edu.ua/xmlui/bitstream/handle/123456789/1749/%D0%9A%D0%B2%D0%B0%D0%BB%D1%96%D1%84%D1%96%D0%BA%D0%B0%D1%86%>

[D1%96%D0%B9%D0%BD%D0%B0%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%B0%20%D0%B1%D0%B0%D0%BA%D0%B0%D0%BB%D0%B0%D0%B2%D1%80%20%D0%9A%D0%B0%](#)

11. Розвиток електронної комерції в умовах глобалізації - URL:

<https://ela.kpi.ua/items/1925ddd3-dc1a-4131-bdcb-5e980beddb11>

E-commerce trends 2024 - URL: [https://www.the-future-of-](https://www.the-future-of-commerce.com/2023/12/20/e-commerce-trends-2024/)

[commerce.com/2023/12/20/e-commerce-trends-2024/](https://www.the-future-of-commerce.com/2023/12/20/e-commerce-trends-2024/)

12. РОЗВИТОК ЕЛЕКТРОННОЇ КОМЕРЦІЇ УПОВІЛЬНИВСЯ У 2024 РОЦІ -

URL: <https://logist.fm/news/rozvitok-elektronnoyi-komerciyi-upovilnivsya-u-2024-roci>

13. ЕЛЕКТРОННА КОМЕРЦІЯ ТА ІНТЕРНЕТ-ТОРГІВЛЯ- URL:

[https://elibrary.kubg.edu.ua/id/eprint/37044/1/Kraus Elektronna komertsii_2021.pdf](https://elibrary.kubg.edu.ua/id/eprint/37044/1/Kraus_Elektronna_komertsii_2021.pdf)

14. Шифрування – що це таке, вимоги GDPR і випадки витоку даних - URL:

<https://www.eset.com/ua/support/information/entsiklopediya-ugroz/shifrovaniye/>

15. ЕЛЕКТРОННА КОМЕРЦІЯ В УКРАЇНІ ТА СВІТІ. ПРОБЛЕМАТИКА ТА ПЕРСПЕКТИВИ 2030 - URL:

[https://ekmair.ukma.edu.ua/bitstream/handle/123456789/20054/Ozhho Elektronna komertsii v Ukraini ta sviti.pdf](https://ekmair.ukma.edu.ua/bitstream/handle/123456789/20054/Ozhho_Elektronna_komertsii_v_Ukraini_ta_sviti.pdf)

17. Дослідження перспектив розвитку електронної торгівлі -

URL: [https://essuir.sumdu.edu.ua/bitstream-](https://essuir.sumdu.edu.ua/bitstream-download/123456789/89428/1/Andrukhov_bac_rob.pdf)

[download/123456789/89428/1/Andrukhov_bac_rob.pdf](https://essuir.sumdu.edu.ua/bitstream-download/123456789/89428/1/Andrukhov_bac_rob.pdf);jsessionid=9EB73D089A67AF1572AF52C3D9B580C4

18. Проблеми електронної комерції в Україні - URL:

<http://dspace.wunu.edu.ua/bitstream/316497/21682/1/%D0%AE%D0%B7%D0%B2%D1%96%D0%BD%20%D0%97%D0%BE%D1%80%D1%8F%D0%BD%D0%B0.pdf>

19. Історія електронної комерції -

URL: https://kztdop.ipf.npu.edu.ua/images/Science/SafetyDey/2020/2020_04_20_History_Money.pdf

20. Управління малим бізнесом у 21 столітті -

URL: https://ukrayinska.libretexts.org/%D0%91%D1%96%D0%B7%D0%BD%D0%B5%D1%81/%D0%9C%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82/%D0%9A%D0%BD%D0%B8%D0%B3%D0%B0%3A%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%D0%BC%D0%B0%D0%BB%D0%B8%D0%BC%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81%D0%BE%D0%BC%D1%83_2_1%D1%81%D1%82%D0%BE%D0%BB%D1%96%D1%82%D1%82%D1%96/04%3A%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9%D0%B1%D1%96%D0%B7%D0%BD%D0%B

[5%D1%81_%D1%82%D0%B0_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%BA%D0%BE%D0%BC%D0%B5%D1%80%D1%86%D1%96%D1%8F/4.02%3A_%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81_%D1%82%D0%B0_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%BA%D0%BE%D0%BC%D0%B5%D1%80%D1%86%D1%96%D1%8F_-](#)

[_%D1%80%D1%96%D0%B7%D0%BD%D0%B8%D1%86%D1%8F](#)

21. СТРАТЕГІЯ РОЗВИТКУ ЕЛЕКТРОННОЇ КОМЕРЦІЇ В ПЕРІОД ПАНДЕМІЇ COVID-19 -

URL:https://www.researchgate.net/publication/350582494_STRATEGIA_ROZVITKU_ELEKTRONNOI_KOMERCII_V_PERIOD_PANDEMII_COVID-19

22. Електронна комерція та її основні виклики: як вашому бізнесу впоратися з кожним із них? - URL:

<https://evergreens.com.ua/ua/articles/ecommerce-challenges.html>

23. Бізнес до бізнесу -

URL:https://uk.wikipedia.org/wiki/%D0%91%D1%96%D0%B7%D0%BD%D0%B5%D1%81_%D0%B4%D0%BE_%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81%D1%83

24. B2C (Бізнес-споживач) - URL:[https://jamkey.com/uk/article/b2c-\(biznes-potrebitel\)](https://jamkey.com/uk/article/b2c-(biznes-potrebitel))

25. Від споживача до споживача -

URL:https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4_%D1%81%D0%BF%D0%BE%D0%B6%D0%B8%D0%B2%D0%B0%D1%87%D0%B0_%D0%B4%D0%BE_%D1%81%D0%BF%D0%BE%D0%B6%D0%B8%D0%B2%D0%B0%D1%87%D0%B0

26. Business to Government (B2G): Selling to The Government -

URL:[https://www.investopedia.com/terms/b/business-to-government.asp#:~:text=Business%20to%20government%20\(B2G\)%20is,%2C%20state%2C%20or%20local%20agencies](https://www.investopedia.com/terms/b/business-to-government.asp#:~:text=Business%20to%20government%20(B2G)%20is,%2C%20state%2C%20or%20local%20agencies).

27. Основи електронного урядування - URL:<https://osvita.kpi.ua/node/413>

28. МОБІЛЬНА КОМЕРЦІЯ - URL:<https://ua.nesrakonk.ru/mobile-commerce/>

29. Соціальні мережі: поняття, історія виникнення. -

URL:<https://zounb.zp.ua/resourse/zaporizkyy-kray/zaporizhzhya-bibliotechne/fahova-osvita/socialni-merezhi-piv>

30. Динаміка зростання аудиторії соціальних мереж: порівнюємо квартальні звіти DataReportal за 2020 і 2021 роки - URL:<https://web-promo.ua/ua/blog/dinamika-rosta-auditorii-socialnyh-setej-cravnivaem-kvartalnye-otchety-datareportal-za-2020-i-2021->

[gody/#%D0%AF%D0%BA%20%D0%A7%D0%B0%D1%81%D1%82%D0%BE%20%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%BE%D0%B2%D1%83%D1%8E%D1%82%D1%8C%20%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96%20%D0%BF%D0%BE%20%D0%B2%D1%81%D1%8C%D0%BE%D0%BC%D1%83%20%D0%A1%D0%B2%D1%96%D1%82%D1%83?](#)

31. Тенденції використання Інтернету у світі - URL:<https://zhuk.ua/istoriyi-ta-fakty/tendentsii-vikoristannya-internetu-u-sviti/>

32. HOW MANY PEOPLE SHOP ONLINE? -

URL:<https://www.oberlo.com/statistics/how-many-people-shop-online>

33. 47+ Online Shopping Statistics For 2024 (Facts & Figures) -

URL:<https://www.demandsage.com/online-shopping-statistics/>

34. Статистика роздрібного товарообігу в Україні -

URL:<https://index.minfin.com.ua/ua/economy/trade/retail/>

35. Mobile Commerce в 2023-2024 роках: основні тренди та рекомендації для онлайн-магазинів - URL:<https://esputnik.com/uk/blog/mobile-commerce-v-2023-2024-rokah-osnovni-trendi-ta-rekomendaciyi-dlya-onlajn-magaziniv>

36. Комплексне дослідження ринку eCommerce - URL:

<https://cases.media/en/case/kompleksne-doslidzhennya-rinku-ecommerce-keis-stylus-kh-promodo>

37. Distribution of internet users worldwide as of February 2024, by age group - URL:

<https://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/>

38. Технічний GDPR: 5 цікавих аспектів - URL:

<https://legalitgroup.com/tehnichnij-gdpr-5-tsikavih-aspektiv/>

39. Концептуальна модель -

URL:https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C

40. Логічна модель даних -

URL:https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D1%96%D1%87%D0%BD%D0%B0_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C%D0%B4%D0%B0%D0%BD%D0%B8%D1%85

41. Коефіцієнт кореляції рангу Кендала - URL:

https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B5%D1%84%D1%96%D1%86%D1%96%D1%94%D0%BD%D1%82_%D0%BA%D0%BE%D1%80%D0%B5%D0%BB%D1%8F%D1%86%D1%96%D1%97_%D1%80%D0%B0%D0%BD%D0%B3%D1%83_%D0%9A%D0%B5%D0%BD%D0%B4%D0%B0%

[D0%BB%D0%B0](#)

42. Баєсова мережа - URL:[https://www.wikidata.uk-](https://www.wikidata.uk-ua.nina.az/%D0%91%D0%B0%D1%94%D1%81%D0%BE%D0%B2%D0%B0%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C.html)

[ua.nina.az/%D0%91%D0%B0%D1%94%D1%81%D0%BE%D0%B2%D0%B0%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C.html](https://www.wikidata.uk-ua.nina.az/%D0%91%D0%B0%D1%94%D1%81%D0%BE%D0%B2%D0%B0%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C.html)

43. Баєсова мережа -

URL:<https://www.wikiwand.com/uk/%D0%91%D0%B0%D1%94%D1%81%D0%BE%D0%B2%D0%B0%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0>

44. Структура Меркла — Дамгора - URL:

<https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B0%D0%9C%D0%B5%D1%80%D0%BA%D0%BB%D0%B0%E2%80%94%D0%94%D0%B0%D0%BC%D0%B3%D0%BE%D1%80%D0%B0>

45. Криптографія з відкритим ключем - URL:

[https://ukrayinska.libretexts.org/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D1%96_%D0%BD%D0%B0%D1%83%D0%BA%D0%B8/%D0%A1%D0%BE%D1%86%D1%96%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F/Cultural_Sociology_and_Social_Problems/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%96%D1%82%D1%8C_%D1%96%D0%BD%D0%B0%D0%BA%D0%BE%D0%BC%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F%3A_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B5_%D0%BF%D1%80%D0%B8%D0%B4%D1%83%D1%88%D0%B5%D0%BD%D0%BD%D1%8F_%D1%82%D0%B0_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%81%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85_%D1%80%D1%83%D1%85%D1%96%D0%B2_\(Borradaile\)/01%3A_%D0%92%D1%81%D1%82%D1%83%D0%BF_%D0%B4%D0%BE_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97/1.07%3A_%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_%D0%B7_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BC](https://ukrayinska.libretexts.org/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D1%96_%D0%BD%D0%B0%D1%83%D0%BA%D0%B8/%D0%A1%D0%BE%D1%86%D1%96%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F/Cultural_Sociology_and_Social_Problems/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%96%D1%82%D1%8C_%D1%96%D0%BD%D0%B0%D0%BA%D0%BE%D0%BC%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F%3A_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B5_%D0%BF%D1%80%D0%B8%D0%B4%D1%83%D1%88%D0%B5%D0%BD%D0%BD%D1%8F_%D1%82%D0%B0_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%81%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D1%85_%D1%80%D1%83%D1%85%D1%96%D0%B2_(Borradaile)/01%3A_%D0%92%D1%81%D1%82%D1%83%D0%BF_%D0%B4%D0%BE_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%97/1.07%3A_%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F_%D0%B7_%D0%B2%D1%96%D0%B4%D0%BA%D1%80%D0%B8%D1%82%D0%B8%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BC)

46. АСИМЕТРИЧНЕ ШИФРУВАННЯ - URL:

https://teletype.in/@technical_science/Asymetric_Crypto

47. Функція Ейлера - URL:

https://ru.wikipedia.org/wiki/%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F_%D0%AD%D0%B9%D0%BB%D0%B5%D1%80%D0%B0

48. Кібербезпека в eCommerce проектах: важливість та шляхи забезпечення - URL: <https://wezom.com.ua/ua/blog/kiberbezpeka-v-proektah-ecommerce-kompleksniy-gayd>
49. SSL-сертифікат - URL: <https://ukeywaf.com/baza/ssl-sertyfikat/>
50. Протоколи електронної пошти - URL: https://help.eset.com/efsw/10.0/uk-UA/idh_config_emon_protocols.html
- SSL & TLS 3: AES and RSA - URL: <https://medium.com/@prateekbansalind/ssl-tls-3-aes-and-rsa-63d356b3ebf7>
51. Что такое криптография с симметричным ключом? Офіційний сайт Binance academy. URL: <https://academy.binance.com/ru/articles/what-is-symmetric-key-cryptography> (дата звернення: 30.10.2020).
52. Bishop D. Introduction to Cryptography with Java Applets. Boston - Toronto - London - Singapore: Jones and Bartlett Publishers, 2003. 387 p.