ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Дослідження методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.»

на здобуття освітнього ступеня магістра
зі спеціальності 122 Комп'ютерні науки
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерні науки
(назва)

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

_____ Андрій ШУЛЯК
(підпис) *(Ім'я, ПРІЗВИЩЕ здобувача)*

Виконав:
здобувач вищої освіти Андрій ШУЛЯК
група КНДМ-61

Керівник: Юрій КАТКОВ
науковий ступінь, вчене звання д.т.н., доцент

Рецензент:
науковий ступінь, вчене звання _____
(Ім'я, ПРІЗВИЩЕ)

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерних наук

Ступінь вищої освіти Магістр

Спеціальність Комп'ютерні науки

Освітньо-професійна програма Комп'ютерні науки

ЗАТВЕРДЖУЮ
Завідувач кафедрою Комп'ютерних наук

_____ Віктор ВИШНІВСЬКИЙ
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Шуляк Андрію Олеговичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce

керівник кваліфікаційної роботи Юрій КАТКОВ д.т.н., доцент,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» 10.2023р. №145
2. Строк подання кваліфікаційної роботи «29» грудня 2023р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література з питань, пов'язаних з теRRAS роботи.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

4.1 Аналіз засобів забезпечення ланцюжків постачання у логістичної компанії THIRD-PARTY LOGISTICS під час E-COMMERCE.

2 Дослідження особливостей забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для E-COMMERCE.

3 Розробка рекомендації щодо застосування інтелектуальних засобів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для E-COMMERCE.

5. Перелік графічного матеріалу: *презентація*

5.1) Тема дипломної роботи

5.2) Мета роботи. Об'єкт дослідження. Предмет дослідження.

5.3) Постановка завдання дослідження.

5.4) Аналіз засобів забезпечення ланцюжків постачання у логістичної компанії THIRD-PARTY LOGISTICS під час E-COMMERCE.

5.6) Рекомендації щодо застосування інтелектуальних засобів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для E-COMMERCE.

6. Дата видачі завдання«19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	19.10-05.11.23	
2	Аналіз специфіки і характеристик основ адміністрування корпоративної мережі	05.11-12.11.23	
3	Дослідження методів здійснення особливостей застосування Windows Server 2022 для адміністрування корпоративної мережі	13.11-19.11.23	
4	Моделювання методів здійснення можливостей Windows Server 2022 у віртуальному середовищі	20.11-25.11.23	
5	Основні розділи.	27.11-03.12.23	
6	Розробка обов'язкових матеріалів.	04.12-10.12.23	
7	Попередній захист роботи.	11.12-20.12.23	
8	Пред'явлення роботи в деканат.	21.12-29.12.23	

Здобувач вищої освіти _____ Андрій ШУЛЯК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій КАТКОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 123 стор., _1_ табл., 45 рис., _58_ джерел.

Наукове завдання – оцінка доцільності та ефективності використання визначених методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Мета роботи – розробка комплексу рекомендацій щодо підвищення ефективності застосування методів безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Об'єкт дослідження – процес застосування методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Предмет дослідження – методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Короткий зміст роботи:

У цій роботі розглядається ключові проблеми кібербезпеки у логістиці та найкращі практики, які можуть допомогти захиститися від кіберзагроз.

1. Виконати загальний аналіз засобів забезпечення ланцюжків постачання у логістичної компанії THIRD-PARTY LOGISTICS під час E-COMMERCE.

2. Виконати дослідження особливостей забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для E-COMMERCE.

3 Виконати розробку рекомендація щодо застосування інтелектуальних засобів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для E-COMMERCE..

КЛЮЧОВІ СЛОВА: ЛОГІСТИЧНА КОМПАНІЯ, БЕЗПЕКА ТА КОНФІДЕНЦІЙНІСТЬ ДАНИХ АДМІНІСТРУВАННЯ,

ABSTRACT

The textual part of the qualifying work for obtaining a master's degree: ____pages, __tables, __figs., __sources.

The scientific task is to evaluate the expediency and effectiveness of using certain methods of ensuring the security and confidentiality of user data in a logistics company for eCommerce.

The purpose of the work is to develop a set of recommendations for increasing the efficiency of the application of security methods and confidentiality of user data in a logistics company for eCommerce.

The object of the study is the process of applying methods for ensuring the security and confidentiality of user data in a logistics company for eCommerce.

The subject of the study is methods of ensuring the security and confidentiality of user data in a logistics company for eCommerce.

Summary of the work:

This paper examines key cyber security issues in logistics and best practices that can help protect against cyber threats.

1. To perform a general analysis of the means of securing supply chains at the logistics company THIRD-PARTY LOGISTICS during E-COMMERCE.

2. Carry out a study of the features of ensuring the security and confidentiality of user data in a logistics company for E-COMMERCE.

3 Develop a recommendation on the use of intelligent means of ensuring the security and confidentiality of user data in a logistics company for E-COMMERCE.

KEY WORDS: LOGISTICS COMPANY, ADMINISTRATION DATA SECURITY AND CONFIDENTIALITY,

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

3PL	-	Логістична компанія Third-Party Logistics
B2B	-	Підприємства продають іншим підприємствам. Часто покупець перепродує продукцію споживачеві.
B2C	-	підприємства продають продукцію окремим споживачам (кінцевим користувачам). Найпоширеніша модель, що має безліч варіацій.
B2G	-	підприємства продають свою продукцію урядам чи урядовим установам
C2B	-	споживачі продають бізнесу. Бізнес C2B дозволяє клієнтам продавати іншим компаніям
C2C	-	споживачі продають іншим споживачам. Компанії створюють онлайн-ринки, які поєднують споживачів
C2G	-	споживачі продають товари урядам чи урядовим установам
G2B	-	уряди чи урядові установи продають бізнесу
G2C	-	уряди чи урядові установи продають споживачам

ВСТУП

У цій роботі розглядаються методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce. Ці методи є основою для вирішення ключових проблем кібербезпеки у логістиці та дозволяють застосовувати найкращі практики, які можуть допомогти захиститися від кіберзагроз за рахунок використання інтелектуальних систем управління логістичними операціями.

Обґрунтування вибору теми та її актуальність. Логістична галузь відіграє ключову роль у світовій економіці, забезпечуючи безперебійне переміщення товарів та матеріалів різними мережами. Логістика стосується загального процесу управління тим, як ресурси отримуються, зберігаються та транспортуються до кінцевого пункту призначення. Ланцюжок постачання створюється постачальниками логістичних послуг, що забезпечують оптимальне і безперебійне функціонування підприємств по всьому світу. Навіть незначна прогалина в каналах постачання та розподілу може зруйнувати життя людей по всьому світу. Несвоєчасне вживання заходів, що коригують, може призвести до втрати як клієнтів, так і бізнесу. Торгові обмеження та недоступність основних продуктів ясно вказують на те, що необхідно ініціювали нові логістичне рішення щодо ланцюжків постачання, наприклад, застосовувати нову інфраструктура та передові технології, отримувати більш повні та наочні дані про логістику, необхідність обмеження витрат. Тому система управління ланцюжками постачання є основою бізнесу успішних підприємств.

Цифрова трансформація логістичної галузі найближчим десятиліттям відкриє нові можливості для бізнесу. Логістична галузь може реалізувати цей потенціал, використовуючи економічно ефективні інтелектуальні технології, оптимізуючи керування процесів постачання, транспортом, впроваджуючи машинні зміни у процеси, такі як складська робототехніка та високошвидкісні залізниці, а також використовуючи програмні рішення, такі як штучний інтелект

та блокчейн. Ці досягнення призводять до різкого збільшення кількості структурованих та неструктурованих даних, які можна аналізувати за допомогою передових технологій, таких як Інтернет речей та штучний інтелект [1, 2 ,3].

Використовуючи рішення Інтернету речей, підприємства можуть досягти більшої прозорості ланцюжка поставок, скоротити операційні витрати та відстежувати товари в режимі реального часу, гарантуючи, що вони прибудуть у потрібний час, місце та у відповідному стані [3, 4, 5].

У 1960-х роках зародилася Концепція бізнес-логістики. На початку 1970-х років вперше був використаний для логістичних компанії термін 3PL- third-party logistics, що займаються інтермодальним маркетингом у транспортних контрактах. 3PL-компанії пропонують обробку замовлень та такі послуги, як складування, комплектування, упаковка та доставка, тобто отримують, обробляють та зберігають товар від торговців. Пізніше термін «сторонній постачальник логістичних послуг» у 1990-х роках, ймовірно, у зв'язку з розвитком технологій, включаючи розвиток Інтернету, трансформувався і визначає особу, яка одноосібно отримує, зберігає або іншим чином транспортує споживчий товар у ході звичайної діяльності, але яка не приймає він право власності на продукт [4, 5].

Сьогодні у зв’язку зі зростання онлайн-продажів і зростання попиту споживачів на більш швидку доставку і нижчі ціни призвели до різкого зростання попиту на 3PL-послуги. Останнім часом є приклади розвитку 3PL в напрямі 4PL. Термін 4PL (Fourth-party logistics) є операційною моделлю, в якій бізнес передає все управління ланцюжком поставок і логістику одному зовнішньому постачальнику послуг. Коротше кажучи, коли 3PL-провайдери передають на аутсорсинг свої послуги за контрактом, вони стають 4PL-провайдерами. Прикладами логістичних компаній у США для доставки електронної комерції є FedEx, UPS, USPS, DHL, Ceva Logistics тощо. Ці логістичні компанії забезпечують внутрішню та міжнародну доставку для онлайн-бізнесу [3, 4, 5].

Однак зі зростанням цифровізації операцій логістичні компанії стикаються зі зростаючою загрозою з боку кіберзлочинців. Кібербезпека стала першорядною

проблемою в галузі логістики, і організації повинні вжити надійних заходів для захисту своїх систем, даних та операцій логістики від шкідливих атак [3, 5].

Нажаль сектор логістики вразливий для різних кіберрисків, включаючи витік даних, атаки програм-вимагачів та збоїв в ланцюжках поставок. Хакери часто використовують уразливості у логістичних системах для отримання несанкціонованого доступу до конфіденційної інформації та порушення операцій. Фішингові атаки зазвичай використовуються для того, щоб обманом змусити співробітників розкрити облікові дані для входу або завантажити шкідливе програмне забезпечення, що наголошує на необхідності обізнаності та навчання співробітників [2, 5].

Безпека ланцюжків постачання є актуальною темою тому що, безпека ланцюжків постачання — це управління процесом постачання, яке фокусується на управлінні ризиками зовнішніх постачальників, продавців, логістики та транспорту. Вона виявляє, аналізує та знижує ризики, що пов’язані з роботою спів сторонніх організацій у рамках ланцюжка постачання. Вона може включати як фізичну безпеку, так і кібербезпеку для програмного забезпечення та пристроїв. Хоча універсальних керівних принципів забезпечення безпеки ланцюжків постачання не існує, повна стратегія вимагає поєднання принципів управління ризиками з кіберзащитою, а також прийняття з урахуванням правових протоколів.

Визначення проблеми. З розвитком інформаційних технологій та їх впровадженням в цифрову економіку розвиваються і методи кібератак на компанії в тому числі і логістичні 3PL/4PL. Індустрія логістики стала однією з цілей для кіберзлочинців. Втручання хакерів у роботу логістичних компаній може спричинити дуже серйозні наслідки. Логістичні компаній регулярно потерпають від хакерів, збитки індустрії рахують у десятках мільйонів доларів.

Треба відмітити, що галузь логістики в цілому рухається недостатньо швидко для вирішення зростаючих проблем у сфері кібербезпеки. Тому виникає проблема кібербезпеки у логістиці щодо пошуку та впровадження найкращих практик, які можуть допомогти захиститися від кіберзагроз [4, 5]..

Кибербезпека в логістика - це захист цифрової ціпочки поставок. Важливість кібербезпеки у логістиці викликана тем, що глобальна логістична мережа утворює складну, взаємозалежну систему, в якій затримки або перебої в одній частині можуть поширюватися по всьому ланцюжку. Кібератаки у логістиці (фішинг, шкідливе програмне забезпечення, програми-вимагачі, інсайдерські загрози та ін.) загрожують цьому тендітному балансу. Кібератака може призвести до значних збоїв у роботі (операційного збою), що викликає фінансові втрати та збитки репутації [2, 4, 5].

Таким чином, ключовими моментами в системі управління ланцюжками постачання є усунення можливих загроз та збоїв, а також вжиття заходів для досягнення найкращих результатів. Аналітика, що підтримується передовими алгоритмами та великими даними, усунула людські обмеження при розрахунку процесу ланцюжка постачання. Компанії, які модернізували свої організації шляхом впровадження цифрових методів прийняття рішень, сьогодні отримують максимальну вигоду з цієї передової тенденції. Більше того, це дозволить краще зрозуміти ймовірності варіантів рішень, допоможе у прийнятті рішень, підвищить продуктивність, забезпечить відстеження у реальному часі та усуне будь-які загрози, що впливають на продуктивність. Тому сьогодні стало очевидним необхідність використання інтелектуальних технологій в електронної комерції для цифрової революції в аналітиці, автоматизації, оцінці та відстеження поставок та логістики в режимі реального часу. Тому забезпечення надійних заходів кібербезпеки захисту цих цифрових ланцюжків поставок — це більше, ніж просто випереджальний підхід — це абсолютна необхідність. Звідси стає зрозумілим актуальність та своєчасність цієї теми [1,2].

Ступінь вивченої проблеми. Ступінь вивченості проблеми на тему «Дослідження методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce» є складним. Проблема кібербезпеки у логістиці досліджується в багатьох аспектах науковцями всього світу [1-7].

Ці дослідження пов’язані з унікальним завданням щодо управління загрозами та ризиками для дуже складних ланцюжків постачання, які підтримують кожну з критично важливих та нових технологій, наприклад, унікальних для штучного інтелекту, зокрема на машинному навчанні, підмножині штучного інтелекту; автономні системи, зокрема, автономні транспортні засоби та інші [1, 2].

Загалом ступінь дослідження проблеми для диплома непростий, але потенційні переваги значні. Це пояснюється тим, що ця тема є відносно новою, та існує не так багато досліджень на цю тему. Ця робота окреслює навички та знання, необхідні для досягнення успіху в цій галузі кіберзахисту логістичних компаній від загроз .

Специфіка джерельної бази. База джерел для диплому є різноманітною та всебічною, охоплює як теоретичні, так і практичні аспекти захисту логістичних компаній від загроз.

Мета роботи – розробка комплексу рекомендацій щодо підвищення ефективності застосування методів безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Об’єкт дослідження – процес застосування методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Предмет дослідження – методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Наукове завдання – оцінка доцільності та ефективності використання визначених методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Завдання роботи:

1. Виконати загальний аналіз засобів забезпечення ланцюжків постачання у логістичної компанії THIRD-PARTY LOGISTICS під час E-COMMERCE.

2. Виконати дослідження особливостей забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для E-COMMERCE.

3. Виконати розробку рекомендація щодо застосування інтелектуальних засобів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для E-COMMERCE..

Методика дослідження. Це дипломне дослідження буде проводитися з використанням підходу змішаних методів, поєднуючи як якісний, так і кількісний збір та аналіз даних. Це дозволяє повністю зрозуміти можливості та проблеми використання визначених методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Результати дослідження. Результати дослідження у цій дипломній роботі розглядають можливості підвищити ефективність застосування методів безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

Апробація результатів досліджень.

Матеріали були опубліковані:

в статті:

Шуляк А.О. Методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії./ Ю. І. Катков, А.О.Шуляк// Наукові записки Державного університету телекомунікацій №4, 2023, Подано до друку. https://journals.dut.edu.ua/index.php/sciencenotes/issue/archive

в тезисах:

Катков Ю. І., Шуляк А. О. МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ // Науково-практична конференція «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ» Збірник тез. – К.: ДУІКТ, 2023. 27 жовтня 2023, С- 365-369. https://duikt.edu.ua/uploads/p_2626_52007398.pdf

1 ЗАГАЛЬНИЙ АНАЛІЗ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЛАНЦЮЖКІВ ПОСТАЧАННЯ У ЛОГІСТИЧНОЇ КОМПАНІЇ ПІД ЧАС E-COMMERCE

1.1 Характеристики електронної комерції (E-COMMERCE)

Електронна комерція (E-COMMERCE) - це засіб продажу товарів та послуг через мережу Інтернет. Визначення бізнесу електронної комерції може також включати таку тактику, як партнерський маркетинг. Електронна комерція - це один із способів, за допомогою якого люди купують і продають речі в роздрібній торгівлі. За оцінками, 2,14 мільярда людей у всьому світі купують товари та послуги онлайн, а кількість учасників Prime, які купують в магазинах Amazon по всьому світу, в даний час перевищує 200 мільйонів [4, 6, 8].

Споживачі можуть використовувати різноманітні канали електронної комерції, такі як власний веб-сайт, авторитетний торговий веб-сайт, такий як Amazon, або соціальних мереж, щоб стимулювати онлайн-продажу. Деякі компанії продають товари тільки через Інтернет, тоді як інші продавці використовують електронну комерцію як частину ширшої стратегії, що включає фізичні магазини та інші канали збуту.

Бізнес електронної комерції - це компанія, яка отримує прибуток від продажу продуктів або послуг через Інтернет. Наприклад, компанія електронної комерції може продавати програмне забезпечення, одяг, товари для дому чи послуги веб-дизайну. Можна вести бізнес у сфері електронної комерції з веб-сайту через декілька онлайн-каналів, таких як соціальні мережі та електронна пошта. Бізнес електронної комерції використовує цифрові методи продажу товарів та послуг клієнтам. Деякі підприємства електронної комерції працюють на 100% цифровій основі, тоді як інші використовують електронну комерцію як

доповнення до звичайного магазину або для розвитку відомих брендів. У будь-якому випадку електронна комерція дозволяє стартапам, малому бізнесу та великим компаніям продавати продукцію у великих масштабах та залучати клієнтів у всьому світі. Підприємства електронної комерції можуть працювати лише онлайн або мати фізичну присутність. Для продажу клієнтам через Інтернет зазвичай потрібний веб-сайт або цифрова вітрина, а також спосіб цифрової обробки платежів та доставки замовлень клієнтам [1, 2]:.

Веб-сайт електронної комерції – це цифрова вітрина бізнесу в Інтернеті. Це полегшує угоду між покупцем та продавцем. Це віртуальний простір де ви демонструєте продукти, а онлайн-покупці роблять вибір. Ваш сайт діє як полиця з продуктами, торговий персонал і касовий апарат вашого онлайн-бізнес-каналу. Компанії можуть створити фірмовий магазин у такому магазині, як Amazon, створити власний комерційний сайт на виділеному домені або зробити все для багатоканального підходу [1, 2, 4].

Маркетинг електронної комерції - це набір стратегій, які ви можете використовувати, щоб направити клієнтів до продуктів та послуг, доступних в Інтернеті. Наприклад, ви можете використовувати маркетинг у соціальних мережах, щоб залучити покупців до інтернет-магазину. Або якщо ви використовуєте рішення для електронної комерції, таке як Amazon, ви можете рекламувати продукти за допомогою платних товарних оголошень (PLA). Дізнайтеся більше в цьому посібнику з маркетингової тактики в електронній комерції [1, 2, 4]. .

Звідси, електронна комерція працює шляхом об'єднання покупців та продавців з використанням різних електронних каналів. Наприклад, використовується канал (веб-сайт або соціальні мережі), щоб клієнти могли знаходити продукти та послуги для покупки. Потім платіжний процесор забезпечує обмін товарів чи послуг. Після успішного завершення транзакції клієнт отримує електронний лист або SMS з підтвердженням, а також квитанцію, яку можна надрукувати. Якщо транзакція стосується товарів, продавець відправляє товари та відправляє покупцеві номер відстеження електронною

поштою або SMS. Якщо транзакція пов'язана з послугою, постачальник послуг може зв'язатися з нею, щоб запланувати та завершити надання послуги.

Види електронної комерції. Електронна комерція приймає стільки різних форм, скільки існує різних способів здійснення покупок в онлайн-каналах. Ось кілька поширених бізнес-моделей, що формують світ електронної комерції [1, 2]:

• B2C – підприємства продають продукцію окремим споживачам (кінцевим користувачам). Найпоширеніша модель, що має безліч варіацій.

• B2B – Підприємства продають іншим підприємствам. Часто покупець перепродує продукцію споживачеві.

• C2B – споживачі продають бізнесу. Бізнес C2B дозволяє клієнтам продавати іншим компаніям.

• C2C – споживачі продають іншим споживачам. Компанії створюють онлайн-ринки, які поєднують споживачів.

• B2G – підприємства продають свою продукцію урядам чи урядовим установам.

• C2G – споживачі продають товари урядам чи урядовим установам.

• G2B – уряди чи урядові установи продають бізнесу.

• G2C – уряди чи урядові установи продають споживачам.

Методи ведення електронної комерції [1, 2, 4]:

- М-комерція.
- Корпоративна електронна комерція.
- Електронна комерція у соціальних мережах.

М-комерція – це онлайн-транзакції на мобільних пристроях. Враховуючи, що портативні пристрої знаходяться в руках споживачів по всьому світу, не дивно, що у 2023 році на мобільну комерцію припадатиме понад 43% від загального обсягу роздрібного продажу електронної комерції (майже на два відсотки більше, ніж у 2022 році). Багато людей зараз вивчають продукти та здійснюють онлайн-покупки через свої телефони. Ця тенденція не демонструє жодних ознак уповільнення, тому дуже важливо оптимізувати свій інтернет-магазин для мобільних пристроїв [1, 2, 5]. .

Корпоративна електронна комерція. Корпоративна електронна комерція – це купівля та продаж продуктів великим компаніям чи організаціям. Якщо великий бізнес продає безліч різних типів продуктів або має кілька лінійок брендів і переходить до продажів через Інтернет, він бере участь у корпоративній електронній комерції [1, 2, 7].

Електронна комерція у соціальних мережах. Соціальні мережі можуть допомогти вам просувати магазини електронної комерції серед широкої аудиторії. Соціальні мережі не лише дозволяють вам спілкуватися з друзями та сім'єю, але й можуть залучити клієнтів до вашого бізнесу. Якщо все зроблено правильно, маркетинг у соціальних мережах приваблює клієнтів у неформальній обстановці [1, 2, 9].

Соціальні мережі можуть допомогти в організації електронної комерції:

• Залучати нових клієнтів.

• Підвищувати впізнаваність бренду.

• Генерувати онлайн-продажі.

Переваги та недоліки електронної комерції [1, 2, 5]. Як і будь-який метод продажу, електронна комерція може мати свої плюси та мінуси. Підходить електронна комерція чи ні залежить від бізнес-цілей, цільової аудиторії та інших факторів [1, 2, 5]..

А) Переваги електронної комерції. Проведення продажів через Інтернет має низку істотних переваг. Серед головних переваг електронної комерції:

• *Швидко росте*. У 2021 році малий і середній бізнес США, що продає в магазині Amazon, експортував понад 225 мільйонів товарів, а міжнародний продаж досяг колосальних 2 мільярдів доларів. Покупці Amazon придбали 3,9 мільярда товарів, приблизно 7500 товарів за хвилину.

• *Пропонує глобальне маркетингове охоплення*. Минулого охоплення бізнесу було обмежено кількістю людей, які могли фізично увійти через двері магазину. Сьогодні електронна комерція дозволяє охопити клієнтів по всьому світу. Зростання використання Інтернету та розвиток соціальних мереж

полегшили власникам бізнесу електронної комерції доступ до нового різноманітного кола клієнтів.

• *Забезпечує зручність замовлення продукції через Інтернет.* Завдяки різноманітності типів електронної комерції клієнти можуть переглядати варіанти та здійснювати покупки з будь-якого місця всього за кілька кліків. Amazon дозволяє легко сортувати та порівнювати товари за ціною або характеристиками. Інновації онлайн-платежів, такі як Amazon Pay, ще більше полегшують процес оформлення замовлення.

• *Передбачає більш низькі експлуатаційні витрати*. Створення та підтримка веб-сайту обходиться дешевше, ніж зміст традиційного звичайного магазину. Можна розпочати бізнес-канал електронної комерції, не орендуючи торговельні площі, не наймаючи команду співробітників та не маючи великого складу. Не потрібно платити орендну плату або турбуватися про обслуговування будинку. Після підключення до Інтернету ваш магазин відкритий 24 години на добу – без необхідності контролю чи укомплектування персоналом, як у звичайному магазині. Можна використовувати інструменти та послуги для створення веб-сайтів, щоб швидко створити власний інтернет-магазин, або ви можете відмовитися від створення веб-сайту та запустити свій бренд у соціальних мережах або в магазині, такому як Amazon. Багато підприємств продають товари через численні онлайн-канали.

• *Забезпечує прямий доступ до споживача*. Завдяки Інтернету бренди електронної комерції можуть безпосередньо вибудовувати стосунки зі своєю аудиторією. Вам не потрібно платити за гігантський рекламний щит або телевізійну кампанію, щоб привернути увагу аудиторії. Ви можете адаптувати свій бренд і маркетинг відповідно до бажань та потреб клієнтів, аж до спеціальних пропозицій та персоналізованих рекомендацій щодо продуктів.

В) Недоліки електронної комерції. Деякі підприємства можуть спробувати уникнути електронної комерції через такі проблеми, як:

• *Обмежене особисте спілкування*. Особиста взаємодія необхідна деяких підприємств і транзакцій. Залежно від вашого продукту, послуги або стилю

продаж може бути складно втілити всю силу вашої особистості в онлайн-просторі. Хоча чарівного рішення немає, збереження історії вашого бренду на чолі всього, що ви робите, може допомогти вам зберегти автентичність в Інтернеті. Альтернативно, якщо ви волієте спілкуватися з клієнтами електронною поштою або телефоном, цей недолік може стати величезним плюсом.

• *Технічні проблеми*. Проблеми, пов'язані з технологіями можуть негативно вплинути на продажі. Так само, як збій у вашому ланцюжку поставок може перешкодити своєчасній доставці продуктів, проблеми з Інтернетом або збій жорсткого диска можуть коштувати вам часу та грошей. Для кожної технічної проблеми, яка може виникнути, напевно знайдеться рішення або профілактичний захід, який ви можете вжити. Обов'язково регулярно створюйте резервні копії даних. Використання такого магазину, як Amazon, допоможе знизити ці ризики завдяки налагодженій і надійній технічній інфраструктурі.

• *Безпека даних*. Клієнтів хвилює, як інформація зберігається та передається. Завойовуйте довіру клієнтів, детально розповідаючи про політику конфіденційності. Це демонструє прозорість і дає клієнтам упевненість у тому, що ви захистите їхню особисту інформацію. В цьому плані протягом десятиліть фахівці працювали над створенням безпечного досвіду покупок, і компанії, які продають, отримують вигоду від багаторічної довіри клієнтів. Коли ви розміщуєте інтернет-магазин у своєму власному домені, вам необхідно знайти безпечну службу обробки платежів і вжити розумних заходів, щоб не наражати на ризик дані клієнтів.

• *Проблеми доставки та виконання замовлень у великих масштабах*. Коли ви починаєте займатися електронною комерцією, може бути легко упаковувати і відправляти замовлення з гаража або вільної кімнати. Але в міру зростання вашого бізнесу виконання замовлень стає набагато більш трудомістким процесом. Несподіване збільшення кількості замовлень може призвести до того, що вам буде складно їх виконати. Використання такої послуги, як Fulfillment від Amazon, може допомогти знизити навантаження на ваш бізнес та забезпечити задоволеність клієнтів.

1.2 Характеристика методів своєчасного виконання замовлення під час електронної комерції

*Своєчасне виконання замовлення***.** Клієнтам потрібна швидкість та ефективність, особливо при здійсненні покупок в Інтернеті. Незалежно від того, що ви продаєте, клієнти хочуть, щоб покупки були доставлені в цілості та безпеці та вчасно.

Фулфілмент (Fulfillment) – це процес доставки продукції клієнтам. Це може включати пошук продуктів, зберігання та упаковку замовлень, обробку повернень та підтримання зв'язку з клієнтами. Успішні магазини електронної комерції приділяють пильну увагу процесу виконання замовлень і стежать за тим, щоб у них було достатньо товарів для виконання замовлень, навіть у найзавантаженіші сезони.

Вибір та реалізація правильних стратегій доставки мають вирішальне значення для успіху будь-якого бізнесу у сфері електронної комерції, тому що клієнти очікують швидкої, зручної та доступної доставки кожного продукту, який вони купують. Більше того, оскільки зростання вашого бізнесу в основному залежить від задоволеності клієнтів, інвестиції в ефективні рішення щодо доставки електронної комерції мають вирішальне значення. Окрім задоволення ваших клієнтів, першокласні стратегії доставки електронної комерції також допоможуть вам збільшити розмір прибутку та підвищити продуктивність вашого бізнесу.

Однак ефективна стратегія доставки виходить за рамки безкоштовної та швидкої доставки. Є й інші чинники, які потрібно враховувати розробки ефективної стратегії доставки електронної комерції.

Важливість доставки електронної комерції. Останнім часом у промисловості електронної комерції спостерігається бум, особливо після пандемії коронавірусу. Безперечно, доставка електронної комерції сьогодні стала основою багатьох компаній. Рішення щодо доставки для електронної комерції відіграють важливу роль у тому, чи здійснює потенційний клієнт покупку чи ні. Безперечно,

важливо забезпечити відмінний досвід покупок, конкурентоспроможні ціни та просування продукції найвищої якості. Але досвід доставки може зрештою вирішити, чи здійснять відвідувачі вашого магазину покупку. Іншими словами, доставка електронної комерції – це основний зв'язок між вами та вашими клієнтами. Якщо ви не згаяєте час на створення системи доставки з ефективними стратегіями, які можуть задовольнити ваших клієнтів, вам буде надзвичайно складно зростати. Ось кілька причин, чому хороша стратегія доставки електронної комерції є важливою для вашого бізнесу:

• Багато брендів постійно вдосконалюють процес доставки. Важливо робити те саме, якщо ви хочете залишатися попереду конкурентів.

• Погано структурований процес доставки в електронній комерції та високі ціни можуть коштувати вам потенційних клієнтів.

• Гарна стратегія доставки допоможе уникнути потенційних проблем. Ви можете обійти проблеми ланцюжка поставок, такі як перевантаження портів або брак робочої сили, співпрацюючи з надійною логістичною компанією.

Більш доступна, ефективна та надійна доставка безпосередньо вплине на ваші коефіцієнти конверсії і, отже, ваш прибуток.

Доставка електронної комерції включає все, що необхідно для доставки продукту з інтернет-магазину до місця призначення його кінцевому споживачеві. Іншими словами, воно включає (Рис.1.1):

Рисунок 1.1 - Доставка електронної комерції.[15]

На Рис.1.1 надані кроки реалізації доставки електронної комерції.

• Приймання замовлень.

• Обробка їх.

• Упаковка купленої продукції на складі.

• Друк етикеток для цих упаковок.

• Надсилання посилок.

• Управління доходами.

Хоча це може здатися відносно простим, кілька рухомих частин створюють набагато складнішу систему, залежно від [12, 15]:

• Розмір вашого бізнесу.

• Тип продукції.

• Розмір продуктів та упаковок.

• Пункти доставки.

Існує безліч стратегій та інструментів доставки в електронній комерції, які допоможуть забезпечити більш ефективну, керовану, швидку та доступну доставку для клієнтів.

Доставка в електронній комерції. Процес доставки в електронній комерції складається з упаковки та доставки.

Існує безліч факторів, які впливають на ефективність процесу доставки вашої електронної комерції. Розглянемо, як доставка електронної комерції має працювати в ідеальному сценарії (Рис.1.2).

Рисунок 1.2 – Етапи доставка електронної комерції [15]

На Рис.1.2 надано три основні етапи доставки електронної комерції [15]:

• *Квитанція замовлення*: на цьому етапі потенційні клієнти будуть переглядати ваш веб-сайт, щоб дізнатися, чи пропонуєте ви продукти, які їм потрібні. Якщо вони знайдуть те, що їм потрібно та хочуть, вони додадуть товари на картку та оформлять замовлення. Щоб виконати ці замовлення, необхідно забезпечити повний контроль над своїми запасами. Це означає, що ви завжди повинні знати, що є, а що ні, і оновлювати цю інформацію на своєму веб-сайті. Використання програмного забезпечення для керування запасами допоможе вам відстежувати свої запаси.

• *Обробка замовлення*: це означає перевірку правильності деталей замовлення від продуктів до адреси доставки та особистої інформації клієнта. Це може усунути такі проблеми, як неправильна адреса доставки або неправильне

написання імені клієнта. Рекомендується максимально автоматизувати етап обробки замовлення, щоб прискорити процес та уникнути людських помилок.

• *Виконання замовлення*: Цей етап означає підготовку замовлення клієнта до надсилання. Підприємствам електронної комерції є кілька варіантів виконання замовлень. Можна виконувати замовлення самостійно або доручити виконання замовлення сторонньому партнеру з логістики (3PL) [16, 24, 27].

Під час доставки електронної комерції виконується відстеження руху замовлення. Для цього існує програмне забезпечення. Надання детальних оновлень відстеження в режимі реального часу – це важливий рівень. Замість того, щоб чекати, поки ваші клієнти пройдуть весь шлях до вашого порталу відстеження, щоб дізнатися, де знаходиться їхнє замовлення, чому б не відправляти оновлення на їх електронну пошту (або номер телефону) кожен раз, коли їх посилка переходить від одного етапу до іншому їм надаються персональні повідомлення. Електронні листи з відстеженням доставки - це хороша можливість додати трохи маркетингу, наприклад програми винагород або навіть навчальні матеріали про продукти, які ви продаєте.

Також є платформа живого чату, призначеної для запитів на доставку. Це спосіб дозволяє відлежувати послуги, щоб усувати неполадки та вирішувати проблеми з відстеженням у режимі реального часу. Це покращуєте якість обслуговування клієнтів при здійсненні покупок.

Способи доставки електронної комерції. Доставка товарів до клієнтів може використовувати різні способи. Наприклад, деякі компанії пропонують лише дводенну доставку, а деякі бренди – нічну доставку. Звичайно бюджет, тип продукції, розмір прибутку та інші фактори будуть впливати на вибір способу доставки (Рис.1.3) [15]:

- Доставка того ж дня.
- 2-денна доставка.
- Нічна доставка.
- Прискорена доставка.

Рисунок 1.3 – Способи доставки електронної комерції.[15]

Доставка того ж дня. Статистика показує, що 61% онлайн-покупців готові доплатити, щоб отримати товари того ж дня, коли вони роблять замовлення. В результаті багато брендів електронної комерції впровадили системи, які забезпечують доставку того ж дня [15, 16, 17].

Плюси:

• Це покращує вашу конкурентну перевагу

• Це дозволяє заробити на імпульсних покупках.

Мінуси

• Це потребує більше зусиль

• Це може стати дорожчим як для вас, так і для ваших клієнтів.

2-денна доставка. Якщо ви не можете запропонувати доставку в той же день, дводенна доставка є найкращим, що ви можете запропонувати. Незалежно від розміру вашого бізнесу у сфері електронної комерції, внесення оперативних змін до процесів доставки може допомогти вам донести цю пропозицію до ваших клієнтів, не перевантажуючи вашу компанію [15, 16, 17]..

Плюси:

• Це дає вам більше часу на підготовку до доставки

• Це покращує якість обслуговування ваших покупців

• Це дешевше, ніж доставка того ж дня.

Мінуси:

• Покупцям доводиться ще почекати, щоб отримати свої товари

Нічна доставка. Цей метод доставки є золотою серединою між доставкою в той же день і доставкою протягом двох днів. Нічна доставка гарантує, що покупці зможуть отримати свої покупки наступного робочого дня [15, 16, 17].

Плюси:

• Це допоможе вам зробити ваших клієнтів щасливими.

• Це спонукає імпульсивних покупців робити покупки.

Мінуси:

• Це потребує більших зусиль щодо планування та логістики.

• Це може бути дорого, залежно від вашого бюджету

Прискорена доставка. Прискорена доставка – це будь-який метод доставки, який забезпечує швидшу доставку, ніж стандартна, гарантуючи, що клієнти отримають свої замовлення якнайшвидше – іноді навіть за кілька годин після розміщення замовлення. Хоча прискорена доставка може виявитися недоцільною для підприємств електронної комерції, що пропонують доставку по всьому світу, вона може мати значення, якщо ви обслуговуєте місцевих клієнтів [15, 16, 17].

Плюси:

• Це допоможе заробити на імпульсивних покупцях.

• Це може зменшити кількість відмов від кошика.

• Це робить ваших клієнтів щасливими

• Це може допомогти вам підвищити лояльність клієнтів

Мінуси:

• Це потребує великих експлуатаційних зусиль

• Це може бути дорогим, залежно від вашого бюджету.

Найкращі інструменти доставки електронної комерції

Процес доставки є одним із стовпів зростання будь-якого бізнесу електронної комерції. Ключовим моментом є інвестування в ефективні та надійні інструменти доставки електронної комерції. Найкращі CMS-платформи для електронної комерції.

CMS (система керування контентом) для електронної комерції – це програмне забезпечення, яке дозволяє власникам бізнесу електронної комерції створювати, адаптувати, удосконалювати та публікувати цифровий контент веб-сайтів без написання коду. CMS – це інтуїтивно зрозуміла інфраструктура, яка дозволяє керувати функціями внутрішнього управління вашого інтернет-магазину, такими як макет сторінки продукту, розділи веб-сайту та багато іншого. Крім того, ваша CMS також може допомогти вам керувати операціями доставки Ось чотири найкращі CMS в електронній комерції на сьогоднішній день [18, 19, 20, 24]:

Shopify. Shopify сьогодні є однією із найбільших платформ електронної комерції. Тим не менш, він також служить платформою CMS і є досить популярним серед власників електронної комерції (понад 2,2 мільйона веб-сайтів). Як CMS Shopify Shipping пропонує просте налаштування вітрини, управління запасами і навіть вбудований кошик для мобільної електронної комерції [18, 19, 20, 24]:.

Плюси:

• Легко використовувати

• Доступні ціни

• Різноманітність привабливих функцій

• Цілодобова підтримка клієнтів

Мінуси:

• Плата за сторонні шлюзи

• Теми налаштовуються лише частково.

• Немає керування кількома магазинами

WooCommerce. Якщо ви хочете перетворити блог WordPress на повноцінний магазин електронної комерції. WooCommerce, мабуть, є найпопулярнішою CMS платформою для власників електронної комерції сьогодні і задовольняє потреби приблизно 28% веб-сайтів електронної комерції у всьому світі. Ця платформа CMS пропонує своїм користувачам широкий вибір розширень та тем. Крім того, WooCommerce також має дуже зручний інтерфейс та просте налаштування розширень [18, 19, 20, 24]:

Плюси:

• Безкоштовна інтеграція з WordPress

• Широкий вибір тем та розширень

• SEO-дружній

• Безпечні платежі

Мінуси:

• Потрібне знання WordPress

• Потрібна окрема оплата як за домен, так і за хостинг.

• Він підтримує лише одну вітрину з одним обліковим записом.

Wix. Хоча Wix є відносно новим доповненням до CMS платформи для покупок в електронній комерції, він швидко став модним. Технічно Wix – це платформа, призначена для допомоги користувачам у розробці веб-сайтів електронної комерції за допомогою інтуїтивно зрозумілих вбудованих інструментів. Але він також непогано справляється із завданням управління. З Wix ви можете швидко створити свій веб-сайт за допомогою вибору естетично привабливих шаблонів платформи та функції перетягування[18, 19, 20, 24]:

Плюси:

• Ніяких знань кодування не потрібне

• Безкоштовний домен на рік

• Доступний

• Інструменти керування запасами та каталогами

• Дозволяє продавати кількома каналами

Мінуси:

• Занадто багато реклами у безкоштовній версії

• Шаблони незмінні після вибору.

BigCommerce. Ця платформа містить широкий спектр вбудованих функцій і настроюваних інструментів, що відповідають потребам CMS. Крім того, BigCommerce також використовує розширену інтеграцію із SEO для підвищення своїх маркетингових результатів. Можна використовувати BigCommerce для кошиків покупок, одночасно використовуючи переваги інших платформ CMS [18, 19, 20, 24]:

Плюси:

• Підтримує продажі кількома каналами

• Пропонує функціональність B2B

• Простий у використанні інтерфейс

• Передові інструменти SEO

• Цілодобова підтримка

• Підтримує багато платіжних шлюзів

Мінуси:

• Менше розширень порівняно з іншими платформами CMS.

• Неможливо легко налаштувати збільшення швидкості сайту.

Програмне забезпечення для електронної комерції. Правильне програмне забезпечення багато в чому допоможе організувати операції з доставки в електронній комерції, структурувати робочі процеси доставки та задовольнити ваших клієнтів швидкою доставкою, відстеженням замовлень і навіть поверненням замовлень, коли це необхідно. Ось список п'яти кращих програм для електронної комерції, щоб ви могли вибрати найкраще для свого бізнесу [18, 19, 20, 24]:

ShipStation. Завдяки своїм привабливим пропозиціям та розширеним функціям ShipStation закріпила за собою місце одного з найкращих програм доставки для власників електронної комерції. ShipStation підтримує інтеграцію з кількома провідними постачальниками електронної комерції та CMS, включаючи

Shopify та BigCommerce. Крім того, ви можете зв'язати свою ShipStation з кількома поштовими перевізниками.

Плюси:

• Пропонує користувачам безкоштовну пробну версію

• Інтуїтивно зрозумілий інтерфейс користувача

• Підтримує понад 350 інтеграцій із постачальниками електронної комерції та доставки.

Мінуси:

• Немає безкоштовних планів

• Обмежені можливості підтримки залежно від вашого плану передплати.

Shippo. Якщо електронна комерція ще не обробляє великі обсяги замовлень, Shippo є відмінним варіантом для вас, оскільки вони пропонують безкоштовний план, який може задовольнити ваші потреби. У безкоштовному плані ви можете платити лише за необхідні транспортні етикетки (п'ять центів за штуку). Однак, транспортні етикетки включені, якщо ви виберете платний план. Крім того, Shippo співпрацює з широким колом міжнародних перевізників та пропонує вражаючі знижки.

Плюси:

• Пропонує безкоштовний план

• Пропонує безкоштовну пробну версію для своїх платних планів.

• Інтегрується майже з сотнею платформ електронної комерції та перевізників.

Мінуси:

• Декілька категорій платних планів

• Обмежена підтримка клієнтів

Easyship Easyship — це ще одне найкраще програмне забезпечення для електронної комерції, особливо якщо міжнародна доставка є важливою частиною вашого бізнесу. Це програмне забезпечення пропонує вигідні знижки на міжнародні кур'єрські служби електронної комерції. Крім того, Easyship дозволяє

заощадити на вартості доставки, надаючи тарифи на доставку в режимі реального часу при оформленні замовлення.

Плюси:

• Пропонує безкоштовний план

• Пропонує 30-денний пробний період для платних пакетів.

• Інтегрується з більш ніж 250 кур'єрськими службами.

• Автоматично оформляє податкові та митні документи

Мінуси:

• Пропонує лише оплату покупок у режимі реального часу для клієнтів із річним планом Shopify.

• Обмежені пропозиції для невеликих пакетів передплати

ShipEngine. Однією з найбільш привабливих особливостей ShipEngine є те, що він пропонує API, що дозволяє оптимізувати процеси доставки та виконання замовлень. Крім того, API-інтерфейси ShipEngine дозволяють порівнювати тарифи на доставку більш як 30 перевізниками в режимі реального часу. Платформа також дозволяє постійно відстежувати доставку вашого замовлення кількома транспортними компаніями електронної комерції.

Плюси:

• Не вимагає жодних контрактів

• Пропонує безкоштовну пробну версію

• Пропонує користувачам безкоштовний обліковий запис розробника.

Мінуси:

• Обмежена інтеграція в порівнянні з іншими платформами

eHub. eHub може підійти вам, якщо ви шукаєте програмне рішення для електронної комерції, яке пропонує вам найнижчі тарифи на доставку щоразу, коли ви хочете відправляти замовлення. eHub виявляє та показує найнижчі тарифи на доставку для кожного замовлення. Таким чином, ви зможете за раз визначити найбільш економічну та найкращу транспортну компанію для вашого інтернет-магазину. Крім того, він пропонує доступ до різних інтеграцій, які допоможуть вам підвищити ефективність доставки.

Плюси:

• Пропонує безкоштовну версію

• Надає безкоштовний пробний період для платних пакетів.

• Інтегрується з численними платформами та операторами зв'язку.

Мінуси:

• Мало можливостей автоматизації.

• Обмежені способи міжнародної доставки.

Перевізники електронної комерції. Знайомство з провідними перевізниками та їхніми послугами у сфері електронної комерції допоможе вам точно налаштувати стратегію доставки. Ось п'ять найкращих варіантів:

USPS. USPS не має собі рівних при доставці до останньої милі. Ймовірно, це пов'язано з тим, що USPS вже щодня здійснює доставку поштових послуг за місцевими маршрутами. Зрозуміло, що це також робить їх одним із найдешевших варіантів наземної доставки.

FedEx. Ще одним провідним перевізником електронної комерції є FedEx. Цей перевізник пропонує своїм користувачам кілька варіантів доставки за різними цінами. Крім того, FedEx також керує FedEx Small Business, метою якого є допомога підприємствам, що ростуть, у задоволенні їх потреб у доставці.

UPS. UPS, безперечно, зарекомендувала себе як один із провідних перевізників електронної комерції. Послуга охоплює широкий спектр напрямків доставки та часу доставки. За допомогою UPS ви можете легко планувати повернення клієнтів.

DHL. Однією з найбільш привабливих особливостей є глобальне охоплення та ефективні послуги міжнародної доставки. Безперечно, це один із найкращих партнерів по доставці для власників електронної комерції.

Royal Mail. Якщо ви перебуваєте у Великобританії і запитуєте, яку кур'єрську службу електронної комерції використовувати, Royal Mail може бути відповіддю. Ця служба пропонує ефективні та швидкі послуги доставки замовлень по Великій Британії та за її межами.

Вартість доставки електронної комерції. Як власник електронної комерції, ви, ймовірно, знаєте, яку роль відіграють ціни на доставку в електронній комерції у визначенні вашого прибутку. Тому цілком логічно, що ви повинні зробити все можливе, щоб дізнатися про вартість доставки та про те, як її можна скоротити [25, 26, 27]:

Види вартості доставки

- Вартість перевезення.
- Вартість упаковки.
- Вартість виконання.
- Накладні витрати.
- Інші витрати.

Вартість перевезення. Це сума, яку стягує ваш перевізник електронної комерції за перевезення вашого замовлення з пункту відправлення до кінцевого пункту призначення.

Вартість упаковки. Ви несете ці витрати, зберігаючи товари, які ви відправляєте своїм клієнтам, у безпечній та надійній упаковці. Такі пакети можуть включати все: від коробок до стрічок, поліетиленових поштових конвертів, кріплення і т.д.

Вартість виконання. Сюди входять витрати на персонал, який збирає, пакує та відправляє замовлення клієнтів.

Накладні витрати. Сюди входять витрати, які вам доведеться сплатити незалежно від кількості або частоти замовлень, які ви відправляєте. Вони включають плату за доставку програмного забезпечення, оренду складу, верстати та обладнання, заробітну плату співробітників і т.д.

Інші витрати. Сюди входять інші витрати, які можуть бути специфічнішими для конкретних замовлень чи незапланованих витрат.

Розрахунок витрати на доставку електронної комерції. Вартість доставки в електронній комерції визначається двома основними факторами [28, 29]:

• Вага та габарити ваших посилок

• Пункт відправлення та пункт призначення

Вага та габарити ваших посилок. Залежно від ваги та розміру посилок, які ви відправляєте, вартість доставки може змінюватись у широких межах. Однак, якщо ваші продукти зазвичай мають однаковий розмір, система цін за одиницю товару може бути найдешевшим способом доставки пакетів електронної комерції. Таким чином, на ціну доставки впливає лише адреса доставки вашого клієнта. Крім того, використання підходу до доставки кожного товару також дозволяє вам пропонувати своїм клієнтам рекламні акції, такі як фіксована ціна за кожне замовлення або відповідні знижки. Незалежно від вашого підходу до цін на доставку, дуже важливо забезпечити точну вагу та розміри ваших товарів. Таким чином, ваш калькулятор доставки електронної комерції завжди буде давати точні результати, і ви уникнете можливих помилок.

Пункт відправлення та пункт призначення. Походження та пункт призначення ваших посилок відіграють важливу роль у визначенні ваших витрат на доставку та стратегії. Залежно від вашої ситуації, ви можете використовувати систему фіксованих тарифів або встановити тарифи в залежності від місцезнаходження адрес доставки ваших клієнтів. Ваш перевізник відіграватиме важливу роль у визначенні вартості доставки в електронній торгівлі, якщо ви здійснюєте міжнародну доставку.

1.3 Характеристики логістичних компанії Third-Party Logistics (3PL), їх операції й функцій

Логістика стосується загального процесу управління тим, як ресурси отримуються, зберігаються та транспортуються до кінцевого пункту призначення. Логістика має вирішальне значення для прибутку компанії. Це забезпечує переміщення матеріалів або товарів, виконання контрактів і надання послуг. Управління логістикою передбачає виявлення потенційних дистриб'юторів і постачальників і визначення їх ефективності та доступності. Менеджерів з логістики називають логістами [18, 19, 20, 24].

Ефективне управління логістикою забезпечує плавний рух по ланцюгу поставок і може забезпечити конкурентну перевагу. Ефективний ланцюжок постачання та ефективні логістичні процедури є важливими для зниження витрат, а також для підтримки та підвищення ефективності. Погана логістика призводить до несвоєчасних поставок, незадоволення потреб клієнтів і, зрештою, завдає шкоди бізнесу.

Мета управління логістикою полягає в тому, щоб мати потрібну кількість ресурсу або вхідних ресурсів у потрібний час, доставити їх у відповідне місце в належному стані та доставити правильному внутрішньому чи зовнішньому клієнту [19, 29]:

У бізнесі логістика - це процес транспортування та зберігання сировини, готової продукції, інвентарю та інших ресурсів. Транспортування та складування - дві основні функції логістичної галузі. Логістика в бізнесі зазвичай складається з багатьох компонентів, включаючи обслуговування клієнтів, прогнозування попиту, складування, обробку матеріалів, контроль запасів, обробку замовлень і транспортування.

Управління транспортуванням фокусується на плануванні, оптимізації та використанні транспортних засобів для переміщення товарів між складами, торговими точками та покупцями. Перевезення є мультимодальним і можуть включати морські, повітряні, залізничні та автомобільні перевезення.

Концепція бізнес-логістики була трансформована з 1960-х років. Зростаюча складність постачання компаній необхідними матеріалами та ресурсами разом із глобальним розширенням ланцюгів постачання призвела до потреби у спеціалістах, відомих як логісти ланцюга постачання. У сучасну епоху технологічний бум і складність логістичних процесів породили програмне забезпечення для управління логістикою та спеціалізовані фірми, орієнтовані на логістику, які прискорюють рух ресурсів уздовж ланцюжка поставок.

Логістичні компанії – це сторонні постачальники послуг з виконання замовлень (також відомі як 3PL- third-party logistics), які пропонують обробку замовлень та такі послуги, як складування, комплектування, упаковка та доставка. Логістичні компанії отримують, обробляють та зберігають товар від торговців.

Термін 3PL вперше був використаний на початку 1970-х років для позначення компаній, що займаються інтермодальним маркетингом у транспортних контрактах. Пізніше термін «сторонній постачальник логістичних послуг» у 1990-х роках, ймовірно, у зв'язку з розвитком технологій, включаючи розвиток Інтернету, трансформувався і визначає особу, яка одноосібно отримує, зберігає або іншим чином транспортує споживчий товар у ході звичайної діяльності, але яка не приймає він право власності на продукт [18, 19, 20, 24].

Сьогодні у зв’язку зі зростання онлайн-продажів і зростання попиту споживачів на більш швидку доставку і нижчі ціни призвели до різкого зростання попиту на 3PL-послуги. 3PL також розквітли завдяки технологіям відстеження, таким як радіочастотна ідентифікація (RFID) та глобальна система позиціонування (GPS), обидві з яких забезпечують розширену прозорість ланцюжка поставок. Тим часом, технологія Інтернету речей (IoT) покращила показники відстеження вантажних перевезень та інших перевізників. Тобто, постачальник 3PL послуг пропонує аутсорсингові логістичні послуги, які включають все, що включає управління одним або декількома аспектами діяльності з закупівель і виконання замовлень. У бізнесі 3PL має широке значення, яке застосовується до будь-якого контракту на обслуговування, що включає зберігання чи доставку товарів. Послуга 3PL може надаватися одним

постачальником, наприклад транспортуванням або складським зберіганням, або бути загальносистемним пакетом послуг, що забезпечує управління ланцюжком поставок .

Основною перевагою використання послуги 3PL для управління логістикою, такої як упаковка, складування, виконання та розподіл, є економія засобів — наприклад, відсутність необхідності утримувати склад чи персонал для моніторингу операцій ланцюжка постачання. Служба 3PL забезпечує більш високу продуктивність при таких операціях як доставка, а також більш легку можливість масштабування своїх операцій.

Останнім часом є приклади розвитку 3PL в напрямі 4PL. Термін 4PL (Fourth-party logistics) є операційною моделлю, в якій бізнес передає все управління ланцюжком поставок і логістику одному зовнішньому постачальнику послуг. Коротше кажучи, коли 3PL-провайдери передають на аутсорсинг свої послуги за контрактом, вони стають 4PL-провайдерами. На відміну від 3PL, який контролює частину операцій ланцюжка поставок для бізнесу, постачальник 4PL зазвичай є єдиною контактною особою для управління ланцюжком поставок. Цей постачальник має ширше коло обов'язків, що включає управління ресурсами, технологіями та інфраструктурою, а також надання стратегічного аналізу та управління. Тобто 3PL-провайдер є менеджером конкретної аутсорсингової послуги, тоді як 4PL-провайдер контролює послуги по всьому ланцюжку постачання. Фактично 4PL-провайдер вибирає та керує різними видами діяльності 3PL, також відомий як провідні постачальники логістичних послуг (LLP - lead logistics providers).

Прикладами логістичних компаній у США для доставки електронної комерції є FedEx, UPS, USPS, DHL, Ceva Logistics тощо. Ці логістичні компанії забезпечують внутрішню та міжнародну доставку для онлайн-бізнесу.

Розглянемо як працює постачальники 3PL та 4PL на наступному прикладі. Нехай є видавництво книг. Видавництво наймає письменників, редакторів та графічних дизайнерів для випуску публікацій, але може не хотіти займатися процесом замовлення споживачами чи транспортуванням партій книг. Натомість

книговидавець використовує центр виконання замовлень для обробки своїх онлайн-замовлень та наймає автоперевізника для перевезення вантажів. Центр виконання та оператор зв'язку виступають як 3PL-провайдери. Один 3PL-провайдер також може виконувати та надсилати замовлення на книги. Уклавши договір з 3PL-провайдером, книжкова компанія може використовувати послуги з постачання та розповсюдження лише за потреби, тим самим більш ефективно контролюючи витрати та одночасно концентруючись на своїй основній компетенції — виробництві книг. Коли 3PL-провайдери передають на аутсорсинг свої послуги за контрактом, вони стають 4PL-провайдерами. У прикладі з книжковим видавництвом, якщо центр виконання передає по субпідряду термозбіжну упаковку та зважування вантажу іншим компаніям, то центр 3PL-провайдера виступає як 4PL-провайдер.

Таким чином, 3PL-провайдери (4PL-провайдери) мають операційною моделлю бізнесу онлайн-продажі конкретної аутсорсингової послугі з постачання та розповсюдження товарів. Дохід 3PL/4PL - провайдерів сьогодні залежить від програмного забезпечення електронної комерції (eCommerce) на ринку управління ланцюжками постачання, оскільки логістичні компанії прагнуть задовольнити потреби в цифровізації. 3PL/4PL - провайдерів починають диференціюватись завдяки інвестиціям у такі технології, як пристрої з підтримкою Інтернету речей, машинне навчання та інтелектуальні машини. Інтернет речей може принести користь постачальникам логістичних послуг з низки причин, включаючи оптимізацію складських потужностей, транспортування, керування працею та безпеку.

Виконання замовлень – одна з ключових частин будь-якого бізнесу у сфері електронної комерції. Швидка та точна доставка замовлень має вирішальне значення для задоволення ваших клієнтів та зміцнення вашої репутації в Інтернеті.

Хоча виконання замовлень власними силами може бути найкращим рішенням для вас на початковому етапі, вам потрібно буде знайти способи підвищити ефективність операцій зі зростанням вашого бізнесу. А логістика

вашого ланцюжка поставок - це те, з чим ви просто не можете дозволити собі недбалість.

Коли ви почнете отримувати дедалі більше замовлень, сторонній постачальник логістичних послуг (3PL) може значно полегшити ваше життя. Цей посібник розповість вам про важливість 3PL для власників бізнесу електронної комерції і навчить вас усьому, що вам потрібно знати про 3PL, щоб ви були готові передати логістику ланцюжка поставок на аутсорсинг.

Як власник магазину електронної комерції, ви, можливо, стикалися із загадковим терміном «3PL». 3PL означає "стороння логістика". Це відносно новий термін, але він набирає популярності, оскільки все більше і більше магазинів електронної комерції усвідомлюють переваги аутсорсингу своїх вхідних та вихідних логістичних операцій.

Стороння логістика (3PL) відноситься до широкої категорії послуг, яка дозволяє підприємствам електронної комерції передавати свої вхідні та вихідні логістичні операції зовнішньому постачальнику, також відомому як постачальник сторонніх логістичних послуг (3PL).

В електронній комерції під вхідною логістикою розуміється процес отримання товарів від постачальників та підготовки їх до розповсюдження.

З іншого боку, вихідна логістика це процес доставки товарів зі складу або розподільчого центру. 3PL подбає про всі ці процеси за вас.

Зокрема, 3PL пропонує послуги з управління запасами, складування та виконання замовлень на національному чи міжнародному рівні від імені своїх клієнтів.

Основна перевага використання 3PL полягає в тому, що вони можуть надати вам ефективніший і послідовніший процес виконання замовлень, ніж ви могли б досягти самостійно.

Приклад архітектури компанії 3PL-провайдери наданий на Рис.1.4

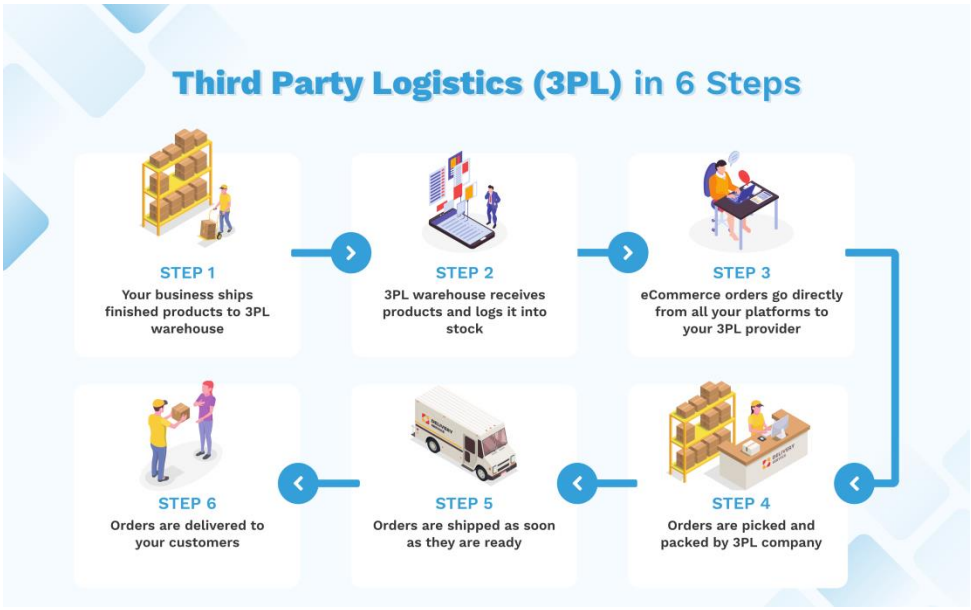


Рисунок 1.4 – Приклад архітектури компанії 3PL-провайдера [29]

Різниця між сторонньою логістикою та виконанням замовлень.

Сторонні логістичні компанії часто плутають із компаніями, які виконують замовлення. Проте вони однакові. Під виконанням замовлень розуміється компанія, яка керує процесом виконання замовлення від початку до кінця, включаючи упаковку та доставку товарів клієнтам.

Основна мета фулфілмент-компанії - забезпечити доставку продукції кінцевому споживачеві в хорошому стані та вчасно. З іншого боку, роль сторонньої логістичної компанії (3PL) полягає в управлінні всім ланцюжком поставок бізнесу їхнього клієнта [27, 28, 29].

Ці компанії часто наймають роздрібні торговці, яким потрібна допомога у вирішенні їхніх завдань у ланцюжку поставок, від управління запасами та складування до доставки. Коли ви користуєтеся послугами стороннього постачальника логістичних послуг для управління логістикою вашого ланцюжка поставок, вам більше не доведеться керувати власними складами або займатися доставкою безпосередньо від постачальників до клієнтів. Натомість ви відправляєте свої замовлення 3PL, який подбає про все інше, включаючи збір товарів з полиць, їх упаковку та відправлення по дорозі [27, 28, 29].

Критична різниця між стороннім постачальником та компанією, що займається виконанням замовлень, полягає в тому, що 3PL беруть на себе весь процес ланцюжка поставок. Навпаки, компанії, які виконують замовлення, займаються лише частиною виконання.

3PL-компанії працює наступним чином (Рис.1.5) [27, 28, 29]:

• Отримання

• Збір

• Упаковка

• Перевезення

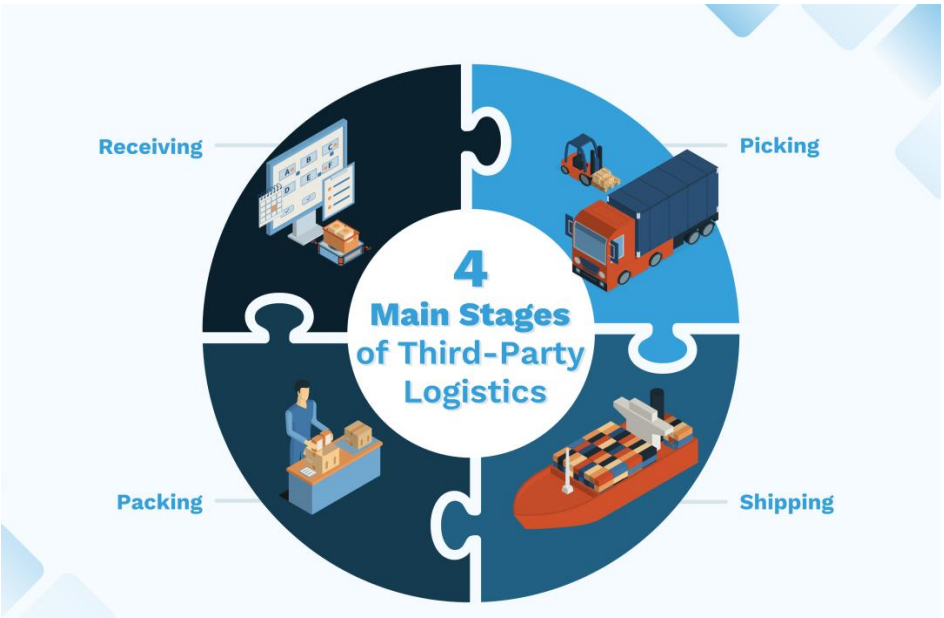


Рисунок 1.5 – Етапи праці компанії 3PL-провайдера [29]

Отримання. Отримання, ймовірно, є найважливішим етапом процесу виконання 3PL. Це тому, що 3PL не зможе доставити ваші товари вашим клієнтам, якщо вони спочатку не отримають вашого інвентарю. І це саме те, що відбувається на цьому етапі процесу: 3PL отримує ваші товари в свій центр виконання замовлень, а потім зберігає їх на своїх виділених складах.

Збір. На етапі комплектації ваш 3PL-провайдер отримує замовлення ваших клієнтів (зазвичай через програмне забезпечення 3PL) і доручає спеціальному співробітнику забирати товари з відповідних складів.

Упаковка. Після того, як ваші товари вибрані для відправки клієнту, настав час їх упакувати. Віддані співробітники вашого 3PL підберуть відповідні варіанти упаковки для ваших товарів залежно від їхньої ваги та розмірів. Вам не потрібно турбуватися про вибір пакувальних матеріалів, оскільки ваш 3PL подбає про це за вас. Пакувальні матеріали зазвичай включають коробки, поштові конверти з бульбашками, пухирчасту плівку, поліетиленові пакети та багато іншого. Деякі 3PL провайдери також дозволяють упаковувати ваші товари у фірмові коробки.

Перевезення. Останній етап процесу виконання 3PL – відвантаження. Ще раз вам не потрібно турбуватися про доставку вашої продукції зі складу до дверей вашого клієнта. Ваш 3PL подбає про все, включаючи етикетки для доставки та вибір кращого перевізника для вас. Деякі 3PL-провайдери працюють зі своїми кращими перевізниками, тоді як інші просто вибирають найбільш доступного перевізника.

Після того, як ваше замовлення буде надіслано, ви отримаєте номер відстеження замовлення, який ви можете повідомити свого клієнта.

Різниця між 1PL, 2PL, 3PL та 4PL логістикою. Стороння логістика (3PL) — це сегмент логістичної галузі, що швидко зростає, який в останні кілька років постійно привертає увагу малого, середнього та великого бізнесу у сфері електронної комерції. Однак, хоча багато власників бізнесу електронної комерції чули термін 3PL, більшість з них не знають, що існує кілька рівнів логістичних послуг, таких як 1PL, 2PL, 3PL та 4PL [30, 31].

Різниця між логістикою 1-ї сторони (1PL), логістикою 2-ї сторони (2PL), логістикою 3-ї сторони (3PL) та логістикою 4-ї сторони (4PL) може спантеличити навіть досвідчених продавців електронної комерції. Але важливо розуміти різницю між цими термінами, оскільки кожен із них належить до різних типів постачальників послуг зі своїми власним набором обов'язків (Рис.1.6).

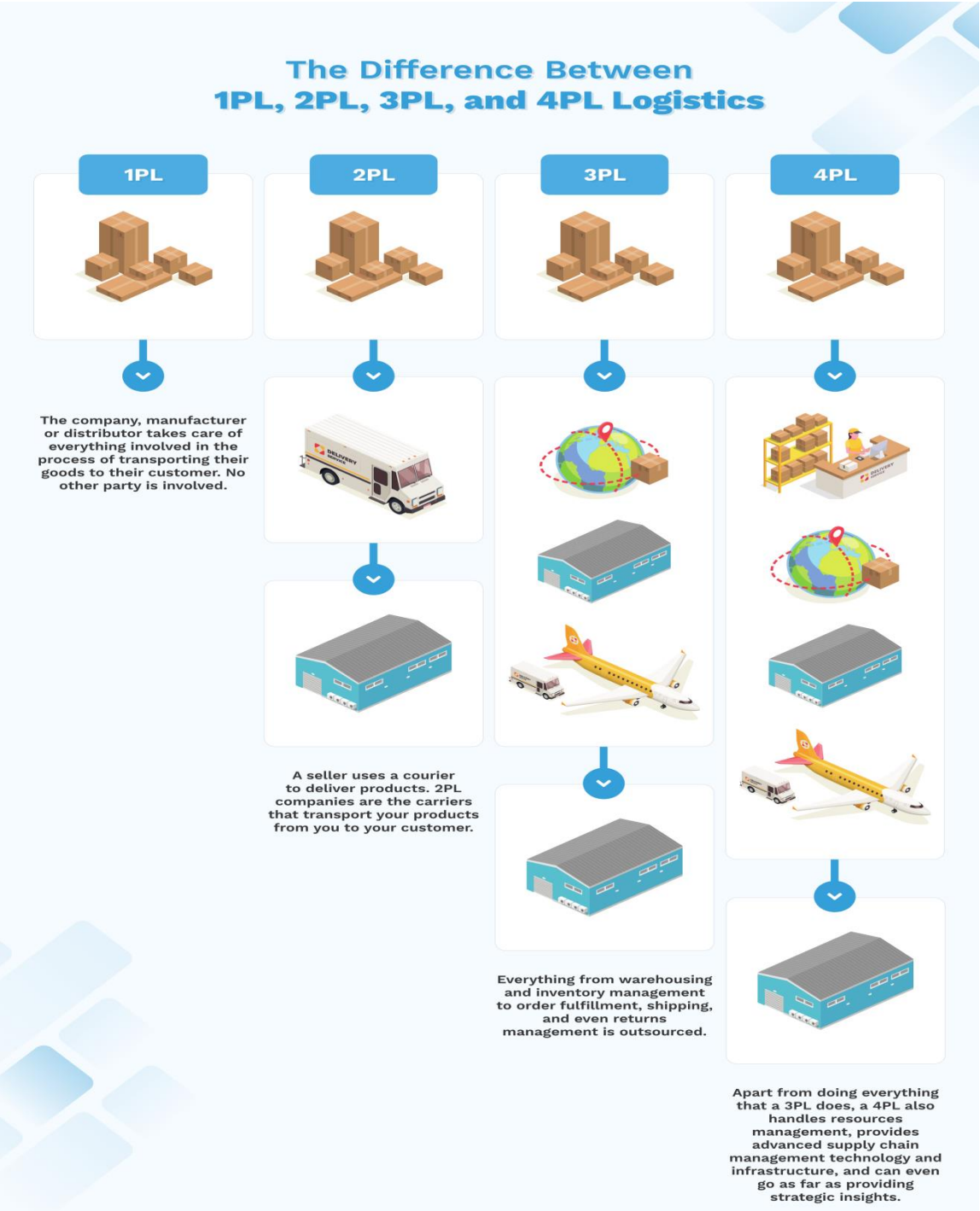


Рисунок 1.6 – Різниця між 1PL, 2PL, 3PL та 4PL логістикою [29]

1PL - Власна логістика. 1PL означає "власна логістика". Цей термін використовується для опису служби доставки, яку компанії пропонують усередині компанії. Вони відповідають за управління всіма аспектами своїх поставок від початку остаточно. Простіше кажучи, у 1PL беруть участь лише дві сторони: компанія, якій необхідно доставити товари, та клієнт, який отримає ці товари. Це

означає, що компанія – виробник чи дистриб'ютор – бере на себе все, що пов'язане із процесом транспортування товару до покупця[30, 31].

2PL – Стороння логістика. 2PL означає вторинну логістику, другий рівень логістики ланцюжка постачання. Він пропонує трохи більш складне рішення, ніж 1PL, оскільки дозволяє передати на аутсорсинг одну з найважливіших частин процесу доставки: транспортування. Коротше кажучи, 2PL компанії - це перевізники, які доставляють вашу продукцію від вас до вашого клієнта. Сюди входять судноплавні лінії, авіакомпанії чи транспортні компанії[30, 31].

3PL – Стороння логістика. 3PL означає сторонню логістику. Як ми пояснювали вище, партнер 3PL допомагає підприємствам електронної комерції керувати переважно операцій у ланцюжку поставок. Це означає, що коли ви наймаєте 3PL, вони подбають про все: від складування та управління запасами до виконання замовлень, доставки та навіть управління поверненнями. Основна перевага найму 3PL-фахівців полягає в тому, що вони візьмуть на себе найважливіші частини операцій вашого ланцюжка поставок, щоб ви могли зосередитися на інших аспектах вашого бізнесу[30, 31].

4PL – Стороння логістика. 4PL означає сторонню логістику і багато в чому схожий на 3PL, але йде крок далі. Як і 3PL, 4PL – це послуга, яка допомагає підприємствам електронної комерції керувати операціями у ланцюжку постачання. Однак основна різниця між 3PL-партнером та 4PL-партнером полягає в тому, що, на відміну від 3PL-партнера, який керує лише частиною операцій ланцюжка поставок, 4PL-партнер керує всім. Це означає, що 4PL просто надає більш технологічні послуги. Крім того, що робить 3PL, 4PL також займається управлінням ресурсами, надає передові технології та інфраструктуру управління ланцюжками поставок і може навіть надати стратегічне розуміння. 4PL – це посередник між вами (бізнесом електронної комерції) та 3PL, який займається управлінням запасами, складуванням, виконанням замовлень та доставкою [30, 31].

Переваги 3PL. У постачальників логістичних послуг є багато переваг. Для багатьох підприємств електронної комерції робота з 3PL стала чарівною

таблеткою для зростання та масштабування їхнього бізнесу, чого в іншому випадку вони не змогли б зробити через обмежені складські площі, недостатній персонал з комплектування та упаковки або інші проблеми з поставками. ланцюгові операції (Рис.1.7) [30, 31].

Рисунок 1.7 – Різниця між 1PL, 2PL, 3PL та 4PL логістикою [29]

Більше свободи. Найбільш очевидною перевагою використання стороннього постачальника логістичних послуг (3PL) є те, що він вивільняє ваш час та ресурси. Всі ці дії забирають багато часу і вимагають вашої пильної уваги. Співпрацюючи з 3PL-провайдером, ви можете легко доручити цю частину свого бізнесу експерту. Без цього навантаження на ваші плечі ви можете зосередитися на маркетингу, продажах, обслуговуванні клієнтів та інших життєво важливих аспектах ведення вашого бізнесу, тоді як вибраний вами 3PL-провайдер займається виконанням замовлень та доставкою.

Не потрібне місце для зберігання. Ще одна величезна проблема для більшості підприємств електронної комерції — місце для зберігання. 3PL подбав про складування, тому вам не обов'язково мати власне. Це означає, що більше не потрібно платити за додаткове місце на складі або платити за додатковий

персонал для керування запасами. Вам також не доведеться турбуватися про те, що ваш нинішній складський простір переросте, тому що 3PL відповідатиме за це за вас.

Швидкі терміни доставки. 3PL бере на себе відповідальність за весь шлях вашого продукту від пункту відправлення до пункту призначення. Щоб зробити цей процес максимально простим, вони мають доступ як до дрібних, так і великих перевізників і можуть доставляти вашу продукцію найбільш ефективним способом. Це часто призводить до скорочення часу доставки, ніж якщо ви відправляли товар безпосередньо зі свого складу.

Економія витрат та підвищення ефективності. Оскільки 3PL-фахівці є експертами у своїй галузі, вони можуть допомогти заощадити час та гроші на експлуатаційних витратах, а також підвищити рівень ефективності вашого бізнесу. е означає, що ви зможете використовувати ці заощадження на свій розсуд — будь то найм більшої кількості співробітників або вихід на нові ринки по всьому світу. Якщо ваш бізнес швидко зростає або починає несподівано розвиватися (що дуже часто зустрічається у сфері електронної комерції), то 3PL може масштабуватись разом з вами без жодних негативних наслідків для операцій. Це означає відсутність фінансових втрат або необхідності призупиняти операції, поки ви шукаєте більш просторе складське приміщення або наймаєте нових співробітників.

Компенсація збоїв у ланцюжку поставок. Управління бізнесом у сфері електронної комерції є досить складним і без необхідності стикатися з перебоями в ланцюжку поставок. Припустимо, аварія на шосе або негода змушують поїзди зупинитися. У цьому випадку це може зіпсувати різні речі у вашому бізнесі, включаючи графіки поставок та запити до служби підтримки клієнтів. Хороший 3PL зможе вирішувати такі проблеми так, щоб вони не впливали на взаємодію ваших клієнтів із вашою компанією.

3PL-послуги. Хороший 3PL-провайдер повинен пропонувати різноманітні послуги, які допоможуть вам доставити товари з заводу до дверей вашого клієнта. Ось найважливіші 3PL послуги [30, 31]:

Складування та управління запасами. Сторонні логістичні компанії є експертами у керуванні вашими запасами та зберіганні товарів. Вони мають склади, де зберігаються товари, які ви продаєте, зазвичай стратегічно розташовані у світі. Якщо ви здійснюєте міжнародне відправлення, 3PL зберігатиме ваші товари на складі, найближчому до вашого клієнта, що допоможе вам скоротити витрати та час доставки. Більше того, 3PL також допоможе вам із керуванням запасами. 3PL-компанії мають знання і досвід для управління всіма частинами процесу управління запасами і зазвичай включають програмне забезпечення для управління запасами. Це може бути особливо корисним, якщо у вас недостатньо місця на власному складі або у вас недостатньо співробітників для контролю над завданнями з управління запасами.

Управління замовленнями та виконання. Коли ви працюєте з 3PL-провайдером, він візьме на себе всі ваші потреби в обробці та виконанні замовлень. 3PL-провайдер буде приймати замовлення від клієнтів, збирати та упаковувати ваші товари та відправляти їх вашому клієнту. 3PL-компанії зазвичай поставляються з розширеною системою управління замовленнями (OMS), яка включає аналіз тенденцій продажів, управління рівнями запасів, управління кількістю запасів в залежності від сезонності, управління кількістю замовлень на основі прогнозів попиту, управління термінами виконання замовлень і багато іншого.

Доставка та розповсюдження. Під доставкою розуміється доставка замовлених покупцем товарів у бажане місце. 3PL-провайдер буде використовувати свою мережу перевізників та об'єктів для доставки продуктів у кінцевий пункт призначення, щоб вони були доставлені якнайшвидше та безпечніше. Постачальники логістичних послуг мають доступ до складів по всій країні, де вони можуть зберігати продукцію доти, доки вона не знадобиться для відправлення, що може значно скоротити час транспортування порівняно з варіантами місцевого складування.

Відстеження замовлення. Відстеження замовлень є найважливішою послугою для будь-якого бізнесу електронної комерції. Це дозволяє вам

відстежувати ваші вантажі та бути впевненими у їх своєчасній доставці. Він також дозволяє дізнатися, де знаходиться ваш вантаж, тому у разі виникнення будь-яких проблем ви зможете негайно їх вирішити. Відстеження замовлень є у більшості 3PL-компаній, і більшість з них пропонують його без будь-яких додаткових витрат для клієнтів. Єдине, що може збільшити ваші витрати на ведення бізнесу, це якщо ви вирішите використовувати систему відстеження замовлень, яка не пропонується вашою 3PL-компанією.

Управління поверненням та обміном. Процес виконання не закінчується доставкою вашої продукції до дверей вашого клієнта. Ось чому більшість 3PL також пропонують повернення та управління обміном. Якщо ваш клієнт не задоволений продуктом і хоче повернути або обміняти його, ваш 3PL подбає про все від зворотної логістики до повернення коштів.

Міжнародна логістика. Якщо ви здійснюєте міжнародні перевезення, 3PL може допомогти вам впоратися з усіма аспектами міжнародної логістики. 3PL можуть допомогти компаніям керувати дистрибуцією в кількох місцях, надаючи складські приміщення у всьому світі або керуючи рівнями запасів у кожному місці на основі поточних прогнозів продажу. Це підвищує ефективність за рахунок мінімізації рівня запасів та забезпечення доступності продуктів у разі потреби.

Види 3PL. Тепер, коли ви повністю розумієте, як працюють 3PL та які послуги вони надають, давайте заглибимося у різні типи 3PL [30, 31]..

Постачальники повного спектру послуг. Якщо ви є магазином електронної комерції, який продає товари по всьому світу і має кілька складів, розташованих у вашій країні походження, ваші витрати на міжнародну доставку будуть неймовірно високими. Припустимо, що вам потрібно доставити посилки клієнтам на інших континентах. У цьому випадку вам знадобиться кілька складів, стратегічно розкиданих по всьому світу, щоб ви могли відправляти свою продукцію зі складу, найближчого до вашого клієнта. Таким чином, ви зможете скоротити витрати на доставку та набагато швидше доставити посилку до дверей вашого клієнта. Саме в цьому вам допоможуть 3PL із повним спектром послуг.

Вони пропонують мережу стратегічно розташованих складів, де зберігатимуть ваші товари.

3PL склади. 3PL склади - найпоширеніший тип 3PL. Ці 3PL компанії зберігають продукти для своїх клієнтів на об'єкті, що належить або орендованому 3PL-компанією. Потім компанія надсилає продукт безпосередньо клієнтам від імені своєї компанії-клієнта. Склади зазвичай розташовані поруч із великими транспортними вузлами, тому можуть швидко доставляти замовлення клієнтам у будь-яку точку світу. Зазвичай вони пропонують послуги швидкої доставки, наприклад протягом одного або двох днів. Це може значно скоротити витрати на доставку та час доставки.

3PL на транспорті. Інший тип 3PL – це 3PL на транспорті. Ці 3PL транспортують ваші товари між вашим заводом та складами. 3PL, засновані на транспорті, пропонують різні транспортні послуги, включаючи автоперевезення, морські та повітряні перевезення.

Фінансові та інформаційні 3PL. У міру того, як ваш бізнес електронної комерції виросте до восьмизначного доходу, операції у вашому ланцюжку поставок стануть набагато складнішими. Саме тоді вам потрібно буде подумати про найм фінансового та інформаційного 3PL. Це найпростіший 3PL. Ці сторонні постачальники логістичних послуг пропонують щось більше, ніж звичайні постачальники послуг 3PL: вони пропонують консультації та галузеву інформацію з управління ланцюжками постачання, щоб ви могли впоратися навіть із найскладнішою логістикою. Вони також забезпечують контроль витрат, аудит вантажних перевезень та технологічно просунуті системи управління запасами.

Ось деякі з найкращих практик забезпечення безпеки даних, що дозволяють зберегти важливість логістики як стратегічної бізнес-функції шляхом захисту ланцюжка постачання від кібератак.

1. Розгортання найкращих у галузі протоколів кібербезпеки. Найважливішою частиною є забезпечення протяжності та широти логістичної мережі за допомогою правильних рішень кібербезпеки та навчання людей.

Логістичні гравці повинні підтвердити, що їхні співробітники знають цінність забезпечення фізичної та кібербезпеки, дотримуючись усіх протоколів, таких як регулярна зміна пароля, відмова від переходу за фішинговими посиланнями, нерозголошення конфіденційної інформації, відмова від хитрощів соціальної інженерії та багато іншого. Також рекомендується скористатися такими рішеннями, як Virtual Unified Threat Management (vUTM) компанії Tata Tele Business Services, яка поєднує критично важливі функції безпеки з розширеними можливостями виявлення вторгнень. Тут важливо регулярно оновлювати та оновлювати програмне забезпечення безпеки, щоб уникнути появи слабких ланок у мережі.

2. Забезпечте видимість глобальної мережі разом із постачальниками. Хоча важко змусити сторонніх постачальників працювати з тим самим рівнем безпеки даних, що й ви, вони також повинні відповідати за дані, які вони обробляють. Цей розсуд передбачає підписання з ними контрактів для забезпечення безпеки інформації та покладання на них юридичної відповідальності за будь-яку компрометовану інформацію. Розгортання програмного забезпечення, що забезпечує прозорість інформації на всіх етапах ланцюжка поставок, також є гарним кроком для виявлення проломів у безпеці та виявлення вразливих точок у мережі.

3. Залучіть партнерів-фахівців з безпеки. Відправлення завжди будуть вразливі для крадіжки – чи то на складі, чи в порту, чи у віртуальних системах. Враховуючи, що щороку втрачаються товари або дані на мільярди доларів, рекомендується наймати спеціалізованих партнерів, які можуть гарантувати безпеку логістичної галузі. Наразі існують спеціалізовані технологічні компанії, які надають передові інструменти для захисту логістики, такі як відстеження контейнерів у реальному часі, безпека мережевих міжмережевих екранів, керування мобільними пристроями, доступ до користувача та багато іншого. Залучення перевірених та авторитетних учасників має вирішальне значення для створення ланцюжка поставок, орієнтованого на створення цінності. Це також дає змогу реалізувати прибуткові стратегії оцінки ризиків.

4. Проводити регулярні перевірки та аналіз безпеки. Регулярне тестування на проникнення та аудит безпеки є відмінними рисами будь-якого успішного налаштування безпеки. Це стосується і логістичної галузі, і логістичних компаній рекомендується наймати «білих хакерів», щоб виявляти слабкі місця у своїх мережах і регулярно усувати їх профілі ризиків. Щорічні або дворічні перевірки безпеки можуть здатися надмірними, але вони можуть мати велике значення для захисту ланцюжка постачання та інтелектуальної власності, якою володіє логістична галузь.

По суті, мета ефективного ланцюжка поставок - доставити сировину з точки А до точки Б найбільш економічним способом. Однак витік даних на будь-якому етапі ланцюжка поставок може призвести до затримок та збільшення витрат на закупівлю. Порушення ланцюжків поставок може завдати значної прямої та непрямої шкоди споживачам та економіці, і це одна з основних причин, чому забезпечення безпеки даних на кожному етапі життєво важливе.

Таким чином, особисті дані, включаючи вік, місцезнаходження, історію покупок, звички купівлі та іншу конфіденційну інформацію, можуть бути легко використані сторонніми брокерами даних для створення докладних цифрових профілів, які вони потім продають іншим організаціям. Логістичні компанії повинні створити спеціальний Команда із забезпечення конфіденційності повинна захищати особисту інформацію, з якою вони працюють. Ця команда має забезпечити суворе дотримання таких правил, як GDPR, SOC2 та інших відповідних міжнародних стандартів.

2 ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ ДЛЯ E-COMMERCE

2.1 Особливості безпеки електронної комерції

Безпека електронної комерції має важливе значення. Кіберзлочинці націлені в основному на підприємства електронної комерції. У 2018 році онлайн-підприємства зазнали 32,4% усіх успішних кібератак. Тому серйозний бізнес має використати надійні протоколи та заходи безпеки електронної комерції. Це захистить бізнес та клієнтів від атак [12, 14].

Безпека електронної комерції є принципом, що забезпечує безпечні транзакції через Інтернет. Він складається з протоколів, які захищають людей, які займаються онлайн-продажем та купівлею товарів та послуг. Вам необхідно здобути довіру клієнтів, впровадивши основи безпеки електронної комерції. До таких основ належать [10, 12, 14].:

• Конфіденційність.

• Чесність.

• Аутентифікація.

• Невідмова від відповідальності.

1. Конфіденційність. Конфіденційність включає запобігання будь-якій діяльності, яка призведе до передачі даних клієнтів неавторизованим третім особам. Крім інтернет-продавця, обраного клієнтом, ніхто інший не повинен мати доступу до його особистої інформації та даних облікового запису. Порушення конфіденційності відбувається, коли продавці надають іншим доступом до такої інформації. Інтернет-бізнес повинен мати щонайменше необхідний мінімум

антивірусів, брандмауерів, шифрування та інших засобів захисту даних. Це буде мати велике значення для захисту кредитних карток та банківських даних клієнтів.

2. Чесність. Цілісність – ще одна важлива концепція безпеки електронної комерції. Це означає, що будь-яка інформація, якою клієнти поділилися в Інтернеті, залишиться незмінною. Принцип свідчить, що онлайн-бізнес використовує інформацію про клієнтів як є, нічого не змінюючи. Зміна будь-якої частини даних призводить до того, що покупець втрачає впевненість у безпеці та цілісності онлайн-підприємства.

3. Аутентифікація. Принцип автентифікації в безпеці електронної комерції вимагає, щоб продавець, і покупець були реальними. Вони мають бути тими, ким вони себе називають. Бізнес повинен довести, що він справжній, займається справжніми товарами чи послугами та виконує те, що обіцяє. Клієнти також повинні надати посвідчення особи, щоб продавець відчував себе в безпеці під час онлайн-транзакцій. Є можливість забезпечити аутентифікацію та ідентифікацію. Якщо ви не можете цього зробити, найм експерта вам дуже допоможе. До стандартних рішень входять дані для входу в систему клієнта та PIN-коди кредитних карток.

4. Невідмова від відповідальності. Відмова означає заперечення. Таким чином, невідмовність - це юридичний принцип, який наказує гравцям не заперечувати свої дії у транзакції. Компанія та покупець повинні довести до кінця ту частину угоди, яку вони ініціювали. Електронна комерція може бути менш безпечною, оскільки вона відбувається в кіберпросторі без живого відео. Невідмовність дає ще один безпековий рівень електронної комерції. Це підтверджує, що повідомлення, яке відбулося між двома гравцями, справді дійшло до отримувачів. Таким чином, сторона в цій конкретній транзакції не може відмовити у підписі, електронному листі чи купівлі.

Ігнорувати безпеку електронної комерції неприпустимо. Хоча зростання електронної комерції покращило онлайн-транзакції, вона однаково привернула

увагу поганих гравців. Звіти про кіберзлочини в електронній комерції показують, що ця галузь є однією з найуразливіших, коли справа стосується кіберзлочинів.

На світ електронної комерції припадає близько 32,4% усіх атак. 50% власників невеликих магазинів електронної комерції скаржаться, що атаки стають дедалі серйознішими. Крім того, звіти показують, що 29% трафіку, що звертається до веб-сайту, складається із шкідливих запитів. Такі атаки призвели до значних втрат у фінансових показниках, частці ринку та репутації. Майже 60% невеликих магазинів електронної комерції, які зазнали кіберзлочинів, не виживають понад шість місяців. Тому дуже важливо вжити надійних заходів безпеки та найняти надійну команду. Це дозволить вам вести свій бізнес, не турбуючись про його закриття через кіберзлочинців.

2.2 Поширені проблеми безпеки електронної комерції

В наступний час відомі такі поширені проблеми безпеки електронної комерції [10, 12, 14]:

1. Нестача довіри до конфіденційності та безпеки електронної комерції.
    - Підроблені сайти.
    - Шкідливі зміни веб-сайтів.
    - Крадіжка даних клієнтів..
    - Збитки комп'ютерних мереж.
    - Відмова в обслуговуванні.
    - Шахрайський доступ до конфіденційних даних.
2. Шкідливе ПЗ, віруси та онлайн-шахрайство.
3. Невизначеність та складність онлайн-транзакцій.

1. Нестача довіри до конфіденційності та безпеки електронної комерції. Підприємства, які здійснюють операції електронної комерції, стикаються з низкою ризиків безпеки, таких як:

• Підроблені сайти. Хакери можуть легко створювати підроблені версії законних веб-сайтів без жодних витрат. Таким чином, постраждала компанія може зазнати серйозних збитків своєї репутації та вартості.

• Шкідливі зміни веб-сайтів – деякі шахраї змінюють вміст веб-сайту. Їхня мета зазвичай полягає в тому, щоб або перенаправити трафік на конкуруючий веб-сайт, або зруйнувати репутацію компанії, що постраждала.

• Крадіжка даних клієнтів. Індустрія електронної комерції сповнена випадків, коли злочинці вкрали інформацію про товарні запаси, особисту інформацію клієнтів, таку як адреси та дані кредитної картки.

• Збитки комп'ютерних мереж – зловмисники можуть завдати шкоди інтернет-магазину компанії, використовуючи атаки хробаків чи вірусів.

• Відмова в обслуговуванні – деякі хакери не дозволяють законним користувачам використовувати інтернет-магазин, що призводить до зниження його функціонування.

• Шахрайський доступ до конфіденційних даних. Зловмисники можуть отримати інтелектуальну власність та вкрасти, знищити чи змінити її у своїх зловмисних цілях.

*2. Шкідливе ПЗ, віруси та онлайн-шахрайство. Ц*і проблеми призводять до втрат у фінансах, частці ринку та репутації. Крім того, клієнти можуть порушити проти компанії кримінальні справи. Хакери можуть використовувати хробаків, віруси, троянські програми та інші шкідливі програми для зараження комп'ютерів та комп'ютерів у різний спосіб. Хробаки та віруси проникають у системи, розмножуються та поширюються. Деякі хакери можуть приховувати троянських коней у підробленому програмному забезпеченні та починати зараження після того, як користувачі завантажують програмне забезпечення. Ці шахрайські програми можуть:

• захоплювати системи комп'ютерів

• стерти всі дані

• заблокувати доступ до даних

• надсилати шкідливі посилання клієнтам та іншим комп'ютерам у мережі.

3. Невизначеність та складність онлайн-транзакцій. Інтернет-покупці стикаються з невизначеністю та складністю під час важливих транзакцій. До таких дій належать оплата, вирішення спорів та доставка. У ці моменти вони можуть потрапити до рук шахраїв. Підприємства підвищили рівень прозорості, наприклад, чітко вказуючи точку контакту у разі виникнення проблеми. Однак такі заходи часто не розкривають повною мірою порядок збирання та використання персональних даних.

2.3 Методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії

Запобігання втраті даних — це рішення безпеки, яке визначає та допомагає запобігти небезпечному чи неналежному обміну, передачі або використанню конфіденційних даних. Це може допомогти компанії контролювати та захищати конфіденційну інформацію в локальних системах, хмарних розташуваннях і кінцевих пристроях. Сховище з вбудованим захистом даних – це системи зберігання даних, які часто включають детальний контроль доступу, що дозволяє обмежити, хто може отримати доступ до ваших даних і за яких обставин. Це може допомогти запобігти несанкціонованому доступу та зберегти конфіденційність вашої інформації. Брандмауер — це пристрій безпеки мережі, який відстежує та фільтрує вхідний і вихідний мережевий трафік на основі попередньо встановлених політик безпеки організації . За своєю суттю брандмауер — це, по суті, бар’єр, який стоїть між приватною внутрішньою мережею та загальнодоступним Інтернетом [10, 12, 14].

Шифрування – це процес захисту інформації або даних за допомогою математичних моделей для їх кодування таким чином, щоб доступ до них мали лише ті сторони, які мають ключ для їх декодування. Платформа захисту кінцевих точок— це рішення, яке розгортається на кінцевих пристроях для запобігання атакам зловмисного програмного забезпечення на основі файлів, виявлення зловмисної активності та забезпечення можливостей розслідування та

виправлення, необхідних для реагування на динамічні інциденти безпеки та попередження [10, 12, 14].

Для застосування цих сучасних технології розроблені наступні методи:

Метод визначення стратегії захисту даних – його застосування життєве важливо для будь-якої організації, яка збирає, обробляє або зберігає конфіденційні дані. Успішна стратегія може допомогти запобігти втраті даних, крадіжці або пошкодженню, а також може допомогти мінімізувати шкоду, заподіяну в разі порушення чи катастрофи. Метод стратегії захисту даних базується на принципах захисту даних, які допомагають захистити дані та зробити їх доступними за будь-яких обставин. Це охоплює оперативне резервне копіювання даних і безперервність роботи/аварійне відновлення, а також включає впровадження аспектів керування даними та доступності даних. Ось ключові аспекти керування даними, що пов'язані із захистом даних[10, 12, 14, 34]:

- Доступність даних — забезпечення доступу користувачів до даних, необхідних для ведення бізнесу, і їх використання, навіть якщо ці дані втрачено або пошкоджено.
- Управління життєвим циклом даних — передбачає автоматизацію передачі критично важливих даних до офлайн- та онлайн-сховищ.
- Управління життєвим циклом інформації — включає оцінку, каталогізацію та захист інформаційних активів з різних джерел, включаючи оцінку збоїв в роботі об'єктів, помилки додатків і користувачів, шкідливі програми та вірусні атаки.

Метод виконання політик (правил) захисту даних. Правила захисту даних регулюють спосіб збору, передачі та використання певних типів даних. Персональні дані включають різні типи інформації, включаючи імена, фотографії, адреси електронної пошти, реквізити банківського рахунку, IP-адреси персональних комп'ютерів і біометричні дані. Правила захисту даних і конфіденційності відрізняються в різних країнах, штатах і галузях. Недотримання закону може призвести до збитків репутації та грошових штрафи залежно від порушення згідно з інструкціями кожного закону та керуючого органу.

Дотримання одного набору правил не гарантує дотримання всіх законів. Крім того, кожен закон містить численні положення, які можуть застосовуватися до одного випадку, але не до іншого, і всі нормативні акти можуть бути змінені. Цей рівень складності ускладнює послідовне та належне впровадження відповідності. Створення правил конфіденційності даних не гарантує, що неавторизовані користувачі не матимуть доступу. Так само ви можете обмежити доступ за допомогою захисту даних, залишаючи конфіденційні дані вразливими. Обидва необхідні для забезпечення безпеки даних. Звідси інша важлива відмінність між конфіденційністю та захистом полягає в тому, хто зазвичай контролює. З міркувань конфіденційності користувачі часто можуть контролювати, якою кількістю їхніх даних ділитися та з ким. Для захисту компанії, які обробляють дані, повинні забезпечити їх конфіденційність. Норми відповідності відображають цю різницю та створені, щоб гарантувати, що запити користувачів щодо конфіденційності виконуються компаніями. Тобто - користувачі контролюють конфіденційність, компанії забезпечують захист. На основі цього методу формуються [10, 12, 33, 34]:

- політика захисту даних;
- стратегія захисту даних;
- визначаються технології та практики захисту даних для захисту приватних даних.

Що стосується захисту даних, користувач може вибрати з багатьох варіантів зберігання та керування. Рішення можуть допомогти: обмежити доступ, контролювати активність і реагувати на загрози.

Для розуміння складності забезпечення безпеки та конфіденційності даних користувача у логістичної компанії ось деякі з найбільш часто використовуваних практик і технологій [10, 12, 33, 34]:

- виявлення даних;
- інвентаризація та класифікація даних;
- відображення даних;

- інструменти автоматизованого виявлення;
- політики запобігання втраті даних;
- моніторинг і сповіщення;
- санація;
- зберігання з вбудованим захистом даних;
- надмірність;
- виправлення помилок;
- контроль доступу;
- резервне копіювання;
- локальні та зовнішні резервні копії;
- інкрементні та повні резервні копії; планування резервного копіювання;
- моментальні знімки;
- миттєве відновлення;
- керування версіями;
- ефективність зберігання;
- тиражування;
- відмово стійкість;
- реплікація даних (відмова);
- балансування навантаження;
- географічна надмірність;
- брандмауери;
- виявлення та запобігання вторгненням;
- контроль додатків;
- моніторинг руху;
- автентифікація та авторизація;
- багатофакторна автентифікація;
- контроль доступу на основі ролей;
- керування ідентифікацією та доступом;

- симетричне, асиметричне та наскрізне шифрування;
- захист кінцевої точки;
- антивірус і захист від шкідливих програм;
- управління пристроєм;
- керування виправленнями;
- стирання даних;
- безпечні методи видалення;
- політика знищення даних;
- сертифікація та аудит;
- аварійного відновлення;
- аналіз впливу на бізнес;
- планування аварійного відновлення;
- тестування та технічне обслуговування та інші.

2.4 Заходи безпеки веб-сайту електронної комерції

В наступний час відомі такі поширені Заходи безпеки веб-сайту електронної комерції [10, 12, 33, 34]:

1. Використовуйте багаторівневу безпеку.
2. Отримайте сертифікати Secure Server Layer (SSL).
3. Використовуйте надійні брандмауери.
4. Дотримуйтесь вимог PCI-DSS.

1. Використовуйте багаторівневу безпеку. Для підвищення безпеки корисно використовувати різні рівні безпеки. Широко поширена мережа доставки контенту (CDN) може блокувати DDoS-загрози та заразний вхідний трафік. Вони використовують машинне навчання, щоб стримувати шкідливий трафік. Також застосовують додатковий рівень безпеки, наприклад, багатофакторну автентифікацію. Хорошим прикладом є двофакторна автентифікація.

Двофакторна автентифікація – це після того, як користувач вводить дані для входу, він миттєво отримує SMS або електронний лист для подальших дій. Реалізуючи цей крок, він блокує шахраїв, оскільки для доступу до облікових записів законних користувачів їм знадобиться щось більше, ніж просто імена користувачів та паролі. Однак злом все одно може статися навіть якщо MFA є. Більшість компаній, які використовують MFA, досі успішно зламуються.

2. Отримайте сертифікати Secure Server Layer (SSL). Однією з основних переваг сертифікатів SSL є шифрування конфіденційних даних, що передаються через Інтернет. Це гарантує, що інформація дійде лише до потрібної людини. Це дуже важливий крок, оскільки всі надіслані дані пройдуть через кілька комп'ютерів, перш ніж їх отримає сервер призначення. Якщо шифрування SSL-сертифіката відсутнє, будь-який електронний пристрій між відправником та сервером може отримати доступ до конфіденційних даних. Таким чином, хакери можуть скористатися вашими відкритими паролями, іменами користувачів, номерами кредитних карток та іншою інформацією.

Таким чином, сертифікат SSL прийде вам на допомогу, зробивши дані нечитаними для непередбачених користувачів.

3. Використовуйте надійні брандмауери. Використовуйте ефективне програмне забезпечення та плагіни для електронної комерції, щоб блокувати ненадійні мережі та регулювати приплив та відтік трафіку веб-сайту. Вони повинні забезпечувати вибіркову проникність, пропускаючи лише довірений трафік. Можна довіряти брандмауеру Astra, щоб зупинити спам, XSS, CSRF, шкідливе ПЗ, SQLi та багато інших атак на ваш сайт. Це гарантує, що єдиний трафік, який отримує доступ до магазину електронної комерції, складається з реальних користувачів. Крім того, ми маємо спеціалізовані рішення WAF для WordPress, Magento, Opencart, Prestashop, Drupal, Joomla, а також PHP-сайти, створені на замовлення. Наприклад, забезпечується захист міжмережевого екрану Astra від:

• 10 основних загроз OWASP

• Захист від поганих роботів.

• Захист від спаму.

• Захист понад 100 типів атак.

3. Антивірусне програмне забезпечення. Сучасним електронним пристроям, комп'ютерним системам та веб-системі необхідна програма або програмне забезпечення, яке виявляє та блокує шкідливе програмне забезпечення, також відоме як шкідливе програмне забезпечення. Таке захисне програмне забезпечення називається антивірусним програмним забезпеченням. Ефективне антивірусне програмне забезпечення має відображати всі приховані шкідливі програми на вашому веб-сайті. Одним з таких сканерів є Astra Malware Scanner. Він цілодобово сканує вашу веб-систему на наявність усіх шкідливих програм і знаходиться у вашому розпорядженні. Він також дозволяє автоматизувати сканування за допомогою функції "Запланувати сканування". За його допомогою можна запланувати сканування щодня, щотижня, щомісяця або раз на два тижні. З Astra Scanner можна отримати:

• необмежену кількість сканувань;

• повідомлення у разі будь-яких змін у файлі;

• сканування з урахуванням машинного навчання;

• колективний розум.

Astra Scanner здатний очищати такі шкідливі програми, як злом кредитних карток, японський спам, pub2srv, фармацевтичні атаки та шкідливі пере направлення. Шкідливе програмне забезпечення WP-VCD відзначено сканером шкідливих програм Astra

4. Дотримуйтесь вимог PCI-DSS. Зробіть обов'язковим дотримання стандарту безпеки даних індустрії платіжних карток (PCI-DSS) для захисту всіх даних кредитних карток. Усі підприємства, що здійснюють транзакції по кредитних картках, повинні дотримуватися таких вимог:

Таким чином, підприємствам слід використовувати кілька заходів та протоколів безпеки електронної комерції, щоб постійно контролювати загрозу безпеці. Крім базових систем аутентифікації, таких як ім'я користувача та паролі, SSL, необхідна багатофакторна аутентифікація.

2.5 Найважливіші інструменти конфіденційності даних для електронної комерції

Конфіденційність даних є найважливішим аспектом електронної комерції, оскільки вона включає збирання, обробку та зберігання конфіденційної інформації від клієнтів, такий як особисті дані, способи оплати та історія покупок. Нездатність захистити ці дані може призвести до юридичних, фінансових та репутаційних втрат, а також до незадоволеності клієнтів та втрати довіри. Таким чином, підприємствам електронної комерції необхідно використовувати ефективні інструменти конфіденційності даних, щоб забезпечити дотримання відповідних правил, таких як Загальний регламент захисту даних (GDPR) та Каліфорнійський закон про конфіденційність споживачів (CCPA), а також для захисту прав та переваг своїх клієнтів. Розглянемо деякі з найважливіших інструментів конфіденційності даних для електронної комерції і те, як вони можуть допомогти керувати своїми даними безпечно та етично[10, 12, 33, 34]:

1. Шифрування даних.
2.Анонімізація даних.
3. Управління згодою на дані.
4. Контроль доступу до даних.
5. Виявлення витоку даних та реагування на неї.
6. Навчання та підвищення обізнаності щодо конфіденційності даних.
7. Моніторинг та виявлення загроз.

1. Шифрування даних. Шифрування даних — це процес перетворення даних у формат, що не зчитається, з використанням секретного ключа, щоб доступ до них могли отримати тільки авторизовані сторони. Шифрування даних має важливе значення для електронної комерції, оскільки воно захищає дані при передачі та зберіганні, не дозволяючи хакерам, кіберзлочинцям та третім особам вкрасти чи підробити їх.

Шифрування даних може застосовуватися до різних типів даних, таких як паролі, номери кредитних карток, адреси електронної пошти та відомості про замовлення. Деякі з найпоширеніших методів шифрування даних для електронної комерції – це Secure Sockets Layer (SSL), Transport Layer Security (TLS) та Advanced Encryption Standard (AES).

Шифрування даних здійснюється завдяки:

• Інструментам шифрування.

• Інструментам виявлення та класифікації даних.

• Інструментам анонімізації та псевдонімізації.

Інструменти шифрування. Інструменти шифрування можуть допомогти компаніям електронної комерції шифрувати дані клієнтів при зберіганні та передачі, роблячи їх нечитаними для тих, хто не має ключа розшифровки. Інструменти виявлення та класифікації даних.

Інструменти виявлення та класифікації даних можуть допомогти компаніям електронної комерції ідентифікувати та класифікувати типи наявних у них даних про клієнтів, наприклад особисті, фінансові чи медичні дані.

2. Анонімізація даних. Анонімізація даних — це процес видалення чи зміни будь-якої ідентифікуючої інформації з даних, таких як імена, адреси, номери телефонів та IP-адреси, щоб її не можна було зв'язати з конкретною людиною. Анонімізація даних корисна для електронної комерції, оскільки дозволяє використовувати дані для аналізу, досліджень або маркетингових цілей, не порушуючи при цьому конфіденційність ваших клієнтів і не порушуючи закони про захист даних. Анонімізація даних може бути досягнута за допомогою різних методів, таких як маскування, хешування, агрегування та узагальнення.

3. Управління згодою на дані. Керування згодою на дані – це процес отримання, зберігання та керування згодою ваших клієнтів на збирання та використання їх даних. Управління згодою на дані також допомагає вам поважати переваги та вибір ваших клієнтів, наприклад, згоду або відмову від певних методів збору даних, доступ або видалення їх даних або відкликання їхньої згоди

у будь-який час. Управління згодою на дані може здійснюватися за допомогою різних інструментів, таких як форми згоди, банери, спливаючі вікна та прапорці.

4. Контроль доступу до даних. Контроль доступу до даних – це процес визначення та забезпечення дотримання того, хто може отримувати доступ, переглядати, змінювати або видаляти ваші дані та за яких умов. Контроль доступу до даних має вирішальне значення для електронної комерції, оскільки допомагає запобігти несанкціонованому або випадковому доступу до ваших даних, який може поставити під загрозу їхню конфіденційність, цілісність і доступність. Контроль доступу до даних також допомагає вам дотримуватись правил конфіденційності даних, таких як GDPR та CCPA, які вимагають від вас обмежити доступ до ваших даних до необхідного мінімуму та вжити відповідних заходів безпеки для їх захисту. Контроль доступу до даних може бути реалізований за допомогою різних інструментів, таких як паролі, біометрія, ролі, дозволи та журнали аудиту.

5. Виявлення витоку даних та реагування на неї. Виявлення витоку даних та реагування на неї – це процес виявлення, локалізації, аналізу та вирішення будь-яких інцидентів, пов'язаних з розкриттям або втратою ваших даних. Виявлення витоку даних та реагування на неї мають вирішальне значення для електронної комерції, оскільки допомагають мінімізувати вплив та наслідки витоку даних, такі як юридичні штрафи, фінансові втрати, скарги клієнтів та збитки репутації. Виявлення витоку даних та реагування на неї також допомагають вам дотримуватись правил конфіденційності даних, таких як GDPR та CCPA, які вимагають від вас повідомляти відповідні органи та ваших клієнтів протягом певного періоду часу, а також вживати відповідних заходів щодо виправлення положення. Виявлення витоку даних та реагування на неї можуть підтримуватись різними інструментами, такими як міжмережні екрани, антивіруси, системи виявлення вторгнень та плани реагування на інциденти.

6. Навчання та підвищення поінформованості про конфіденційність даних. Навчання та підвищення поінформованості про конфіденційність даних – це процес навчання та інформування ваших співробітників, партнерів та клієнтів про важливість, принципи та практику конфіденційності даних. Навчання та обізнаність щодо конфіденційності даних мають важливе значення для електронної комерції, оскільки вони допомагають вам створити культуру конфіденційності даних у вашій організації, а також зміцнити довіру та лояльність серед ваших клієнтів. Навчання та поінформованість про конфіденційність даних також допоможуть вам дотримуватись правил конфіденційності даних, таких як GDPR та CCPA, які вимагають від вас продемонструвати свою підзвітність та відповідальність за свою діяльність з обробки даних. Навчання та підвищення обізнаності щодо конфіденційності даних можна проводити за допомогою різних інструментів, таких як онлайн-курси, вебінари, інформаційні бюлетені та політики.

*7. Моніторинг та виявлення загроз***.** Для захисту логістичної компанії від грабіжників і пожеж є надійний засіб - моніторинг та виявлення загроз. Надійні замки та сигналізація здаються надійним рішенням на випадок крадіжки зі зломом. Але що, якщо зловмисник непомітно викраде ваш ключ і код сигналізації і таким чином отримає доступ до вашого офісу в будь-який час? У такому випадку зловмисник може обійти всі запобіжні заходи, тому необхідна система виявлення, наприклад, камера. Подібні проблеми виникають і з безпекою цифрових систем. Цифрові зловмисники також гарантують, що вони можуть легко повернутися без необхідності повторного проникнення. Складність сучасних цифрових систем і величезні обсяги даних означають, що превентивні заходи безпеки все частіше не можуть гарантувати безпеку системи.

Моніторинг та виявлення безпеки вирішує цю проблему. Наприклад, він може виявити, що ноутбук має дуже регулярне і часте з'єднання із зовнішнім світом, що може свідчити про зараження шкідливим програмним забезпеченням. Оскільки це може мати багато причин і потрапляти на ноутбук різними

способами, боротися з цим за допомогою профілактичних заходів практично неможливо. Моніторинг та виявлення безпеки намагається виявити такі патерни якомога швидше за допомогою алгоритмів, щоб запобігти або мінімізувати негативні наслідки, такі як витік даних або програми-вимагачі. Якість виявлення кібератак залежить від якості алгоритмів.

3 РОЗРОБКА РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ ДЛЯ E-COMMERCE

3.1 Рекомендації щодо застосування інтелектуальних засобів для розробки веб-сайту електронної комерції

Дані - це життєдайне джерело будь-якого бізнесу, і одна помилка в їхньому захисті може призвести до величезних втрат для бізнесу. Тому забезпечення безпеки даних є критично важливим. Java, яку часто вважають універсальною, потужною та популярною об'єктно-орієнтованою мовою програмування, допоможе вам забезпечити бездоганну безпеку, якої не може запропонувати більшість мов програмування. Вона відіграє ключову роль у зміцненні безпеки даних і системи, не вимагаючи при цьому ніякого технічного жаргону.

Java - це програмна мова, яка була вперше представлена компанією Sun Microsystems у 1995 році. Вона використовує об'єктно-орієнтований підхід до програмування і надійно працює на різних платформах завдяки віртуальній машині Java (JVM).

Основні характеристики Java включають:

1. Об'єктно-орієнтована парадигма: Java використовує концепцію класів та об'єктів, що спрощує розробку та обслуговування коду.

2. Мультиплатформеність: Завдяки JVM, Java дозволяє виконувати код на різних платформах без перекомпіляції.

3. Безпека: Використання віртуальної машини сприяє високому рівню безпеки, обмежуючи доступ та запобігаючи виконанню небезпечного коду.

4. Автоматичне управління пам'яттю: Java надає автоматичне управління пам'яттю для запобігання витокам та проблемам з вказівниками.

5. Багатофункціональні бібліотеки: Широкий набір стандартних бібліотек полегшує роботу з різними аспектами програмування.

6. Широке застосування: Java використовується для розробки мобільних додатків, веб-додатків, корпоративних систем та вбудованих пристроїв.

Завдяки Java мільйони пристроїв працюють бездоганно. Її перевага над іншими мовами полягає в тому, що вона має унікальні та безпечні функції. Java більш безпечна тому, що:

1. Програми на Java виконуються всередині пісочниці (своєрідної віртуальної машини).

2. Вона пропонує пакет "java.security", який реалізує явну безпеку.

3. Він не дозволяє використовувати явні вказівники.

4. Включає байт-кодовий верифікатор для перевірки фрагментів коду на наявність нелегального коду.

5. Виконує динамічні перевірки безпеки під час завантаження коду та багато іншого.

Java дотримується принципу WORA ("напиши один раз, запускай будь-де"), який підтверджує, що заходи безпеки послідовно застосовуються на різних платформах, від серверів до настільних комп'ютерів і навіть мобільних пристроїв. Це як мати універсальний ключ, який підходить до кожного замка.

Java - найкращий вибір, особливо для компаній, які покладаються на передачу даних між кількома вузлами. Вона забезпечує безпечний зв'язок через мережі, захищаючи дані під час передачі.

Java пропонує надійні бібліотеки шифрування, які підтримують передові методи шифрування, за допомогою яких розробники можуть реалізувати бездоганну безпеку. Це означає, що ваша конфіденційна інформація залишається недоступною для сторонніх очей.

Автентифікація є основою безпеки системи. Java включає в себе безліч методів автентифікації для забезпечення високого рівня безпеки - від комбінацій

імені користувача та пароля до багатофакторної автентифікації. Це гарантує, що доступ до системи отримають лише потрібні користувачі. Надійна автентифікація та авторизація повинні бути пріоритетними при розробці програмного забезпечення на Java для усунення порушень.

Розуміння важливості безпеки в бізнесі створює основу для усвідомлення того, чому Java є цінним союзником:

1. Незалежність від платформи та досвід шифрування:

2. Незалежність Java від платформи гарантує однаковий захист безпеки для різних систем та гаджетів. Це означає, що ваші методи захисту працюють без збоїв незалежно від того, чи використовуєте ви стаціонарний комп'ютер, чи мобільний пристрій.

3. Java пропонує надійні бібліотеки для шифрування даних, що робить її ефективним варіантом для захисту конфіденційних даних. Для ваших цифрових активів це все одно, що мати непроникне сховище.

Надійна автентифікація - вона пропонує кілька типів автентифікації, щоб переконатися, що доступ мають лише дозволені користувачі. Це схоже на слідчого на дверях, який перевіряє посвідчення особи, перш ніж дозволити доступ.

Функції безпеки Java діють як укріплена фортеця для вашого додатку, захищаючи ваш бізнес від потенційних загроз та вразливостей. Ось короткий огляд того, як Java сприяє безпеці вашого бізнесу:

1. Перевірка байт-коду.

Це одна з основних функцій Java, яка допомагає підвищити безпеку додатків. Вона гарантує, що код, який працює на JVM (віртуальній машині Java), дотримується протоколів безпеки, не даючи шкідливому коду прослизнути крізь щілини.

2. Менеджери безпеки.

Java дозволяє вам використовувати менеджерів безпеки для встановлення обмежень на різні можливості Java-додатків. Це все одно, що призначити пильних охоронців, які стежитимуть за відвідувачами та встановлюватимуть обмеження.

3. Завантажувачі класів.

Допомагає перевірити, чи завантажені класи є надійними та перевіреними. Уявіть собі пильного сторожа, який все перевіряє, а потім впускає в дім лише авторизованих гостей.

4. Криптографія:

Java пропонує потужні бібліотеки криптографії, що дозволяють легко шифрувати та розшифровувати дані. Таке шифрування діє як непроникний щит, гарантуючи, що навіть у випадку несанкціонованого доступу дані залишаться нерозбірливими.

5. Автентифікація та авторизація.

Java надає надійні механізми автентифікації та авторизації, що дозволяє вам перевіряти ідентифікацію користувачів та контролювати їхній доступ до даних.

3.2 Рекомендації щодо управління доступом до даних на веб-сайту електронної комерції

Дані - один з найцінніших активів для будь-якого бізнесу. Щоб захистити конфіденційну інформацію, потрібно не лише обмежити доступ до даних, які знаходяться в різних хмарах і середовищах, але й перевірити автентичність осіб, які намагаються отримати доступ до цих даних.

Контроль доступу до даних - це фундаментальний інструмент безпеки, який дозволяє обмежувати доступ на основі набору політик. Впроваджуючи надійні політики доступу до даних, ви допомагаєте захистити персональні дані (PII), інтелектуальну власність та іншу конфіденційну інформацію від потрапляння в чужі руки, як всередині організації, так і ззовні.

Існує чотири основні моделі застосування контролю доступу до даних:

1. *Дискреційний контроль доступу (DAC)*: Найменш обмежувальна модель контролю доступу до даних, DAC покладається на власника або адміністратора ресурсу або на рішення про те, хто має дозвіл на доступ. Ця модель є

децентралізованою, що дає користувачам можливість ділитися доступом з іншими та ускладнює контроль за тим, хто має доступ до конфіденційної інформації вашої компанії. У моделі DAC кінцевий користувач - наприклад, особа, яка створює файл або папку - має повну свободу дій щодо встановлення привілеїв доступу, а також передачі прав доступу іншим користувачам. Ця модель має деякі невід'ємні проблеми з безпекою, такі як вразливість до троянських коней та інших атак шкідливого програмного забезпечення.

2. *Обов'язковий контроль доступу (MAC)*: У цій моделі, що не передбачає дискреції, кінцевий користувач не має жодного контролю над налаштуваннями дозволів. Центральний орган, наприклад, адміністратор або власник, контролює доступ, встановлює, змінює та відкликає дозволи. У моделі MAC доступ ґрунтується на класифікації даних і рівні допуску або формального схвалення доступу, який мають користувачі. Цей підхід, яким може бути складно керувати, широко використовується у військових організаціях.

3. *Контроль доступу на основі ролей (RBAC)*: Доступ у цій моделі надається на основі набору дозволів, які залежать від рівня доступу, необхідного певній категорії користувачів для виконання своїх повсякденних обов'язків. За допомогою RBAC різні працівники отримують різні привілеї доступу на основі таких критеріїв, як посадові функції та обов'язки. Широко використовувана система RBAC поєднує в собі призначення ролей з повноваженнями та дозволами. Вона розроблена навколо заздалегідь визначених ролей, які визначаються за такими критеріями, як центр витрат, бізнес-підрозділ, індивідуальні обов'язки та повноваження. Коли особа змінює обов'язки, роботу або функції, адміністратор призначає цьому користувачеві нову роль, яка заздалегідь визначена в системі.

4. *Контроль доступу на основі атрибутів (ABAC)*: Динамічна модель управління доступом до даних, ABAC надає доступ на основі як атрибутів, так і умов середовища, які включають такі фактори, як місцезнаходження та час. Ці атрибути та умови призначаються як користувачам, так і даним або іншим ресурсам. ABAC забезпечує більшу гнучкість у порівнянні з RBAC, оскільки ви

можете змінювати атрибути та їхні значення без необхідності змінювати суб'єкт-об'єктні відносини. Це означає, що коли ви приймаєте нові рішення про доступ, ви можете динамічно змінювати елементи керування доступом.

Щоб спростити управління контролем доступу до даних, багато організацій впроваджують таку платформу, як управління ідентифікацією та доступом (IAM). Переваги використання рішення IAM включають в себе наступні:

1. Централізований та уніфікований контроль над даними у вашій організації.

2. Автоматизовані завдання, такі як забезпечення.

3. Спрощена відповідність нормативним вимогам, таким як GDPR, HIPAA, PCI та CCPA.

Загальний регламент про захист даних є одним із найсуворіших і найширших заходів захисту даних у світі. Запроваджений у травні 2018 року, Загальний регламент захисту даних був розроблений і написаний Європейським Союзом (ЄС). Однак дотримання GDPR впливає на міжнародні організації, розташовані в будь-якій точці світу, якщо вони мають справу з суб'єктами даних, що базуються в країнах-членах ЄС. Основні зміни в GDPR стосуються кількох категорій, зокрема, розширення територіальної сфери дії, прав суб'єктів даних, а також штрафних санкцій. Територіальна сфера дії тепер поширюється на організації з країн, що не є членами ЄС, які обробляють дані громадян ЄС, а права суб'єктів даних зобов'язують організації повідомляти про порушення щоразу, коли воно відбувається. Крім того, завдяки застосуванню суворих штрафів, таких як 4% від річного глобального обороту організації або 20 мільйонів євро (залежно від того, яка сума є більшою), організації постійно готуються до виконання цього нового регламенту.

HIPAA (Health Insurance Portability and Accountability Act) - це законодавство Сполучених Штатів, яке забезпечує конфіденційність і безпеку даних для захисту медичної інформації. В останні роки цей закон набув більшої популярності у зв'язку з численними витоками медичних даних, спричиненими

кібератаками та атаками з вимогами викупу на медичних страховиків і постачальників послуг.

Стандарт безпеки даних індустрії платіжних карток або **PCI DSS** - це набір стандартів безпеки, який розроблений і адмініструється Радою зі стандартів безпеки індустрії платіжних карток для регулювання обробки конфіденційних платіжних даних клієнтів.

Каліфорнійський закон про захист персональних даних (California Consumer Privacy Act, CCPA) належить до хвилі нових нормативних актів про захист даних, натхненних GDPR. Він схожий на GDPR у тому сенсі, що не обмежується якоюсь конкретною галуззю, а це означає, що незалежно від місцезнаходження вашого бізнесу, він повинен відповідати новому регламенту.

Однак, якщо GDPR вимагає дотримання вимог від усіх організацій, незалежно від їхнього розміру та діяльності, то CCPA застосовується лише до підприємств, які перевищують річний поріг доходу, або тих, які обробляють певну кількість персональних даних.

Безпека даних настільки ж складна, наскільки й важлива. Оскільки ваше середовище стає складнішим, а загрози еволюціонують, особливо важливо послідовно впроваджувати політики доступу до даних. Розгляньте рішення, яке може спростити процеси контролю доступу до даних, одночасно підвищивши рівень безпеки за допомогою додаткового рівня, який відстежує зловмисний або несанкціонований доступ.

3.3 Рекомендації щодо псевдонімізації, шифрування та анонімізація даних на веб-сайту електронної комерції

GDPR (новий закон Європейського Союзу про захист даних) визначає **псевдонімізацію** як обробку персональних даних таким чином, що дані більше не можуть бути пов'язані з конкретним суб'єктом даних без використання додаткової інформації. Зберігаючи деідентифіковані дані окремо від "додаткової інформації",

GDPR дозволяє обробникам даних більш вільно використовувати персональні дані, не боячись порушити права суб'єктів даних. Це пов'язано з тим, що дані стають ідентифікованими лише тоді, коли обидва елементи зберігаються разом.

Псевдонімізація перетворює конфіденційне поле даних на псевдовипадковий рядок (звідси і назва). Отриманий рядок завжди однаковий для одних і тих самих вхідних даних, тому аналітичні кореляції все ще залишаються можливими. Цей процес також називають "токенізацією даних".

Псевдонімізацію можна налаштувати (або ініціалізувати) за допомогою цифрового секретного ключа, щоб тільки ті, хто має доступ до цього секретного ключа, могли псевдонімізувати вхідні дані в той самий вихід. Це означає, що зовнішній зловмисник без секретного ключа не зможе вгадати псевдонімізовану форму листа, навіть якщо він знає початковий незахищений лист. Крім того, ви можете періодично змінювати це секретне значення, щоб ще більше посилити захист конфіденційності даних.

Анонімізація - це незворотне видалення інформації, яка може призвести до ідентифікації особи, або на основі видаленої інформації, або в поєднанні з іншою інформацією. Це визначення підкреслює, що анонімізовані дані повинні бути позбавлені будь-якої інформації, що дозволяє ідентифікувати особу, що унеможливлює отримання інформації про неї, навіть тією стороною, яка відповідає за анонімізацію.

Приховування або маскування даних є крайньою формою анонімізації. Вона замінює інформацію заздалегідь визначеним фіксованим текстом (або чорною стрічкою). Маскування даних дуже просте в реалізації і дуже ефективне у видаленні конфіденційних даних. З іншого боку, в процесі маскування втрачається будь-яка статистична або аналітична цінність даних.

Шифрування переводить дані в іншу форму, щоб їх могли прочитати лише люди або система, яка має доступ до секретного ключа (який офіційно називається "ключ дешифрування"). Згідно зі статтею 32 GDPR, контролери зобов'язані впроваджувати ризик-орієнтовані заходи для захисту безпеки даних.

Одним із таких заходів є "шифрування персональних даних", яке "робить дані нерозбірливими для будь-якої особи, яка не має дозволу на доступ до них".

Існує дві основні схеми шифрування даних: симетричне шифрування та асиметричне шифрування:

1. Симетричне шифрування має слабку сторону - наявність секретного ключа на стороні шифрування, який за своєю суттю важко захистити. Будь-яка особа (наприклад, системний адміністратор), що має доступ до виробничої системи, може викрасти секретний ключ і використовувати його для розшифрування даних. Хоча існують деякі апаратні рішення, цю проблему складно вирішити.

2. Асиметричні схеми шифрування, такі як RSA, DSA або ECC, використовують два ключі: відкритий і закритий. Для шифрування даних використовується відкритий ключ, і навіть якщо зловмисник отримає цей ключ, він не зможе розшифрувати захищені дані. Асиметричне шифрування, однак, набагато повільніше, ніж симетричне, і з цієї причини воно рідко використовується для шифрування даних самостійно.

Мета гомоморфного шифрування - дозволити обчислення зашифрованих даних. Гомоморфне шифрування - це форма шифрування, яка дозволяє обчислювати зашифровані дані, генеруючи зашифрований результат, який при розшифровці відповідає результату операцій, як якщо б вони були виконані над вихідними даними. Практичне застосування гомоморфного шифрування ускладнюється низкою проблем, оскільки система повністю гомоморфного шифрування ще не розроблена. Обмеження в основному базуються на тому, як математичні функції підтримуються над зашифрованими даними. Сподіваємося, що з часом ця ситуація покращиться.

3.4 Рекомендації щодо застосування біометричної технології та ідентифікації користувача на веб-сайту електронної комерції

Біометрія - це форма безпеки, яка використовує різні фізичні характеристики людини для підтвердження ідентифікації. До них відносяться відбитки пальців, сканування райдужної оболонки ока, малюнок сітківки та розпізнавання обличчя. Коли користувач намагається увійти в систему або потрапити в зону з обмеженим доступом, біометричні дані використовуються для швидкого і точного підтвердження особи. Біометрична автентифікація часто є більш безпечною, ніж звичайні методи автентифікації, оскільки вона спирається на інформацію, яка є дуже специфічною для кожної людини.

Біометрична автентифікація користувачів зазвичай використовується для входу в захищений обліковий запис в Інтернеті або для відкриття замкнених дверей чи воріт. Проте, вона все частіше інтегрується і в повсякденну електроніку. Приватні корпорації та державні установи все ще використовують технології біометричної автентифікації на контрольно-пропускних пунктах і прикордонних переходах. Нижче наведені приклади широко використовуваних методів біометричної автентифікації користувачів:

1. Розпізнавання обличчя - ця система порівнює обличчя користувача з базою даних попередньо перевірених облич на основі різних вимірів і атрибутів.

2. Сканер відбитків пальців - відбитки пальців скануються, щоб зафіксувати характерні візерунки гребенів і завихрень.

3. Сканери очей - доступні сканери райдужної оболонки та сітківки ока. Сканери райдужної оболонки ока використовуються для ідентифікації людей шляхом аналізу унікальних візерунків на їх райдужній оболонці. Світло від сканера сітківки направляється на око, де стають видимими індивідуальні особливості кровоносних судин сітківки.

4. Розпізнавання голосу - потрібно багато вимірювань голосу людини, щоб створити унікальний "голосовий відбиток", який може бути використаний для пошуку збігів у базі даних.

Перш ніж дозволити комусь або чомусь доступ до приватних даних або систем, автентифікація гарантує, що це саме той, за кого себе видає особа. Вона необхідна для запобігання несанкціонованому доступу, оскільки обмежує доступ до даних лише тими, хто має на це право.

Без автентифікації інформація є вразливою до крадіжки, фальсифікації або злому, оскільки будь-хто може отримати до неї доступ. Автентифікація може захистити від багатьох ризиків безпеки, включаючи фішинг, хакерство та соціальну інженерію. На щастя, ймовірність цих ризиків, а також необхідність захисту конфіденційної інформації та активів можна значно зменшити, запровадивши автентифікацію. Для перевірки ділової активності можна використовувати різні підходи, включаючи традиційні комбінації імені користувача/пароля, одноразові паролі, токени безпеки та біометричні ідентифікатори, такі як відбитки пальців і розпізнавання обличчя. Ці процедури інтуїтивно зрозумілі та достатньо гнучкі, щоб задовольнити індивідуальні потреби.

Автентифікація дозволяє зафіксувати, коли і хто отримав доступ до певного ресурсу. Компанії повинні визначати, хто винен у витоку даних або в іншій події, пов'язаній з безпекою. Компанії можуть значно покращити свій стан безпеки за допомогою аудиту та підзвітності, а також забезпечити дотримання нормативних вимог. Також вона дозволяє компаніям відстежувати, хто і коли отримав доступ до приватних даних. За допомогою цих даних можна виявити та усунути потенційні прогалини в безпеці. Підзвітність та аудит також можуть бути використані для виявлення моделей поведінки, які можуть становити загрозу безпеці, що дозволяє вжити превентивних заходів.

Завдяки автентифікації підвищується довіра та надійність. Завдяки цьому зберігається конфіденційність даних і захищається добре ім'я компанії. Коли бізнес використовує надійні механізми автентифікації, партнери, клієнти та інші зацікавлені сторони з більшою ймовірністю довіряють йому.

Надійні методи автентифікації дозволяють компаніям показати споживачам та іншим зацікавленим сторонам, що вони дбають про захист конфіденційності

особистої інформації клієнтів. Підвищення лояльності та довіри клієнтів може в кінцевому підсумку призвести до збільшення обсягів бізнесу та зміцнення позицій на ринку.

Незважаючи на зростаючий інтерес до технологій біометричної автентифікації, їх широке поширення стримується низкою моментів, які потребують роз'яснення. Ось три найпоширеніші хибні уявлення про біометричну автентифікацію:

1. Біометрія вторгається в приватне життя.

2. Статичні зображення та фотографії можуть обдурити біометричну ідентифікацію.

3. Термін дії біометричних моделей закінчується з віком або зміною характеристик.

3.5 Рекомендації щодо захисту від витоків інформації та несанкціонованого доступу на веб-сайт електронної комерції

Хоча витік даних - це несанкціоноване використання даних з вашої організації до зовнішнього джерела, більшість витоків даних відбувається випадково. Наприклад, електронний лист, що містить пароль, може бути випадково доставлений не тому одержувачу, що надасть несанкціонований доступ цьому користувачеві. Користувач не обов'язково має зловмисні наміри.

Це на відміну від витоку даних, який зазвичай є навмисним і зловмисним. Іноді, однак, різниця не очевидна, оскільки першим кроком зловмисників є витік даних. Лише після того, як зловмисники отримують доступ до конфіденційної інформації, вони можуть використовувати її у зловмисних цілях, і тоді це вже вважається витоком даних.

Типи витоку даних:

1. Людські помилки. Слабкі облікові дані співробітників, неправильні конфігурації та надмірні дозволи дозволяють отримати доступ до конфіденційної інформації.

2. Застаріле програмне та апаратне забезпечення. Якщо ви не оновлюєте програмне та апаратне забезпечення, ваша мережа та інфраструктура можуть бути незахищеними та неправильно сконфігурованими, що може бути використано зловмисниками для витоку даних.

3. Фізична крадіжка. Знімні USB-накопичувачі, викинуті документи, вкрадені або загублені ноутбуки - все це може стати джерелом витоку даних у майбутньому, якщо до фізичного приміщення організації буде здійснено злом.

4. Внутрішні джерела. Незадоволені працівники або колишні працівники зі зловмисними намірами можуть здійснити витік даних заради фінансової вигоди (наприклад, атаки з вимогою викупу) або з метою помсти організації.

5. Ризик третіх осіб. Якщо ваші треті сторони не дотримуються належних внутрішніх практик безпеки, ваші дані також можуть опинитися під загрозою.

6. Шкідливі електронні повідомлення. Соціальна інженерія, шкідливе програмне забезпечення та фішинг - це атаки на кібербезпеку з високим ступенем успіху в розкритті конфіденційних даних.

Хороша новина полягає в тому, що витоку даних часто можна запобігти, запровадивши правильну політику безпеки. Такі заходи можуть включати в себе наступне [35, 36, 37]:

1. Впроваджуйте заходи безпеки даних. Організації повинні впроваджувати заходи безпеки даних, такі як шифрування даних, багатофакторна автентифікація, обмеження прав доступу та підхід до безпеки на основі нульової довіри, як першу лінію захисту для запобігання витоку даних. Додаткові політики безпеки, такі як видача працівникам ключових карток, можуть запобігти фізичній крадіжці, яка призводить до витоку конфіденційних даних.

2. Запровадьте обов'язкове навчання з кібербезпеки. Навчання співробітників допомагає всій організації працювати разом і розуміти типи

людських помилок (наприклад, слабкі паролі та надмірні дозволи), які вони контролюють, і використовувати ці знання для кращого захисту від кібератак.

3. Захистіть свої кінцеві точки. Настільні комп'ютери, мобільні телефони, ноутбуки та пристрої Інтернету речей - все це точки входу, які зловмисник може використати для отримання доступу до мережі вашої організації. Передача даних через електронну пошту та USB-пристрої також є поширеною точкою входу для зловмисників.

4. Використовуйте засоби запобігання втраті даних (DLP). Існує безліч комерційних інструментів, які виявляють витік даних. Інструменти DLP часто поєднують різні методи захисту, такі як захист кінцевих точок, служби моніторингу, антивірусне програмне забезпечення та передові рішення, які включають машинне навчання та штучний інтелект для виявлення та захисту від втрати та витоку даних.

5. Відстежуйте ризики, пов'язані з третіми сторонами. Оскільки треті сторони є одним з найпоширеніших джерел витоку даних, постійний моніторинг їх має вирішальне значення. Цього вимагають багато галузевих нормативних актів та інструкцій, які покладають на вашу організацію відповідальність у разі витоку даних третьою стороною.

3.6 Рекомендації щодо захисту від соціально-інженерних атак на веб-сайт електронної комерції

Соціальна інженерія - це кібератака, коли злочинці психологічно маніпулюють користувачами, які нічого не підозрюють, щоб змусити їх припуститися помилок у системі безпеки та розкрити свою конфіденційну інформацію. Інженерія полягає в тому, що злочинець використовує людські емоції, такі як страх, цікавість, жадібність, гнів тощо, щоб обманом змусити жертву перейти за шкідливим посиланням або здійснити фізичну атаку.

Зловмисники, які використовують соціальну інженерію, переслідують одну з двох цілей:

1. Вони хочуть зіпсувати дані, щоб спричинити незручності для організації.

2. Вони хочуть вкрасти інформацію, гроші або отримати небажаний доступ.

Ось невеликий перелік найпоширеніших шахрайських схем соціальної інженерії, які застосовуються проти сучасних підприємств та приватних осіб (Рис.3.1):

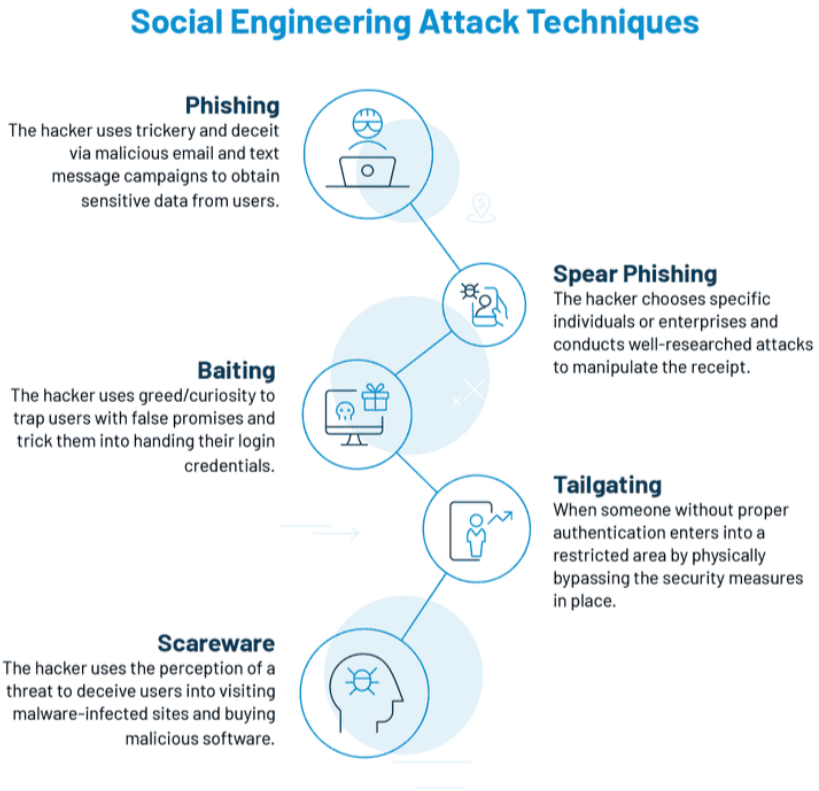


Рисунок 3.1 – Види соціально-інженерних атак на веб-сайт електронної комерції [38]

1. Фішинг.

Фішинг - найпоширеніша та найуспішніша форма атак соціальної інженерії. Шахрай використовує хитрість і обман через електронну пошту, чат, веб-рекламу або веб-сайт, щоб переконати людину або організацію розкрити свої персональні дані та інші цінності. Наприклад, шахрай може видавати себе за представника банку, урядової організації або великої корпорації, якій довіряє наївна жертва. Джерелом може бути електронний лист із проханням до одержувачів натиснути

на посилання для входу до свого облікового запису. Потім їх перенаправляють на фальшивий веб-сайт, який виглядає легітимним, і саме там відбувається атака.

2. Списовий фішинг.

Списовий фішинг - це ще одна форма соціальної інженерії, коли шахрай збирає інформацію про особисте та професійне життя жертви, щоб створити потрібний привід. Наприклад, шахрай може повідомити жертві, що вона планує влаштувати сюрприз на день народження для друга і шукає допомоги, щоб його здійснити.

3. Заманювання.

Приманка - це коли шахрай використовує жадібність або цікавість жертви, щоб заманити її в пастку неправдивими обіцянками та обманом змусити передати свої облікові дані для входу в систему. Наприклад, шахрай може залишити заражену шкідливим програмним забезпеченням флешку (або приманку) в найменш підозрілому місці, наприклад, у туалеті або ліфті компанії. Приманка також матиме привабливі ярлики, як-от платіжна відомість або оціночний лист, які будуть досить спокусливими, щоб вставити їх у комп'ютер.

4. Програми залякування.

Залякування - це тактика шкідливого програмного забезпечення, коли шахрай сприймає загрозу як обман, щоб змусити користувачів відвідати заражені сайти та придбати шкідливе програмне забезпечення. Прикладами можуть слугувати програми перевірки працездатності комп'ютера та оновлення антивірусів, які залякують жертв, змушуючи їх купувати непотрібні їм діагностичні та ремонтні послуги.

Будьте обережні з тим, чим ви ділитеся. І ні, не потрібно ставати параноїком через ці атаки. Запобігти їм можливо. Нижче наведено кілька способів, які допоможуть:

1. Встановіть високий рівень фільтрів спаму. Кожна поштова програма має фільтри спаму. Щоб дізнатися про це, уважно перегляньте параметри налаштувань і встановіть їх на найвищому рівні. Це допоможе вам значною мірою захиститися від спаму.

2. Ніколи не використовуйте один і той самий пароль для різних акаунтів. Якщо зловмисник отримає доступ до одного акаунта, він зможе зламати й інші акаунти.

3. Використовуйте двофакторну або багатофакторну автентифікацію. Простого пароля вже недостатньо для захисту вашого акаунта. Додаткові рівні просто необхідні. Це може бути секретне питання, капча, відбитки пальців або коди підтвердження за допомогою SMS.

4. Якщо ви сумніваєтеся, негайно змініть пароль. Якщо ви вважаєте, що передали свій пароль спамеру, негайно змініть всі свої паролі.

5. Навчайте своїх знайомих. Знання - це ключ до успіху. Інформуйте своїх близьких або знайомих про останні загрози соціальної інженерії та допомагайте їм проявляти необхідну обережність, коли це необхідно.

3.7 Розробка Web-Додатку для логістичних компаній з використанням аутентифікації та авторизації користувача

3.7.1 Налаштування середовища розробки. Перш ніж почнемо налаштування середовища розробки, потрібно налаштувати Maven конфігурацію. Почнемо з налаштування Maven. Це можливо зробити або за допомогою сайту “Spring initializr” або власноруч, створюючи файл pom.xml з залежностями та плагінами. (Рис.3.2):

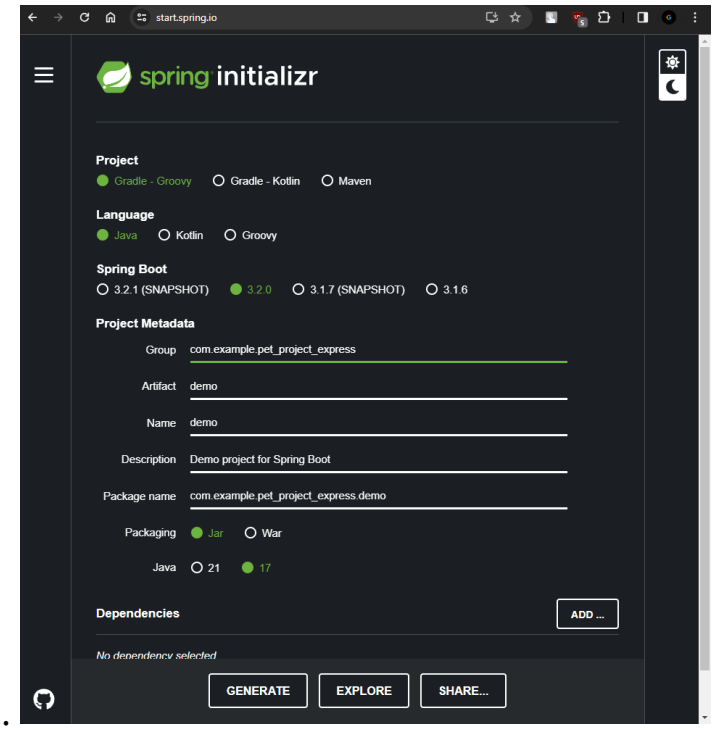


Рисунок 3.2 — Налаштування Spring initializr [38]

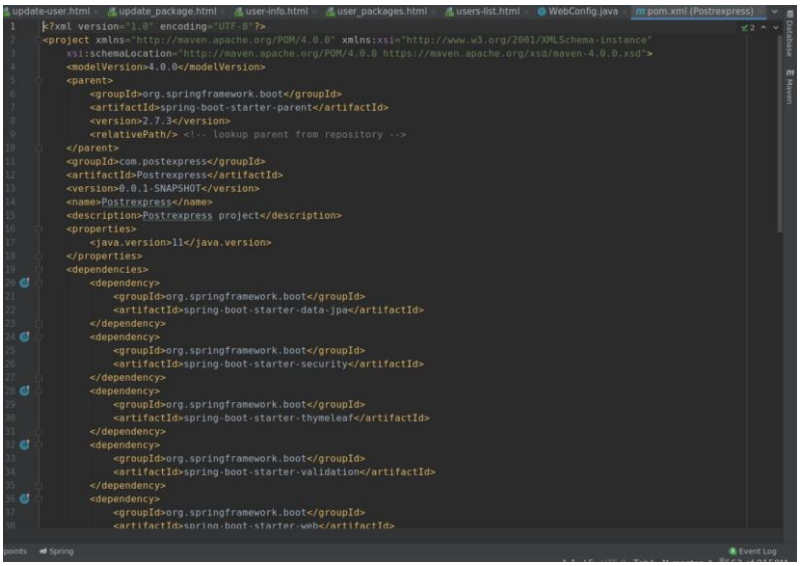


Рисунок 3.3 — Конфігурація файлу pom.xml [38]

3.7.2 Конфігурація бази даних перед початком роботи з проектом. Налаштування бази даних у Java Spring може залежати від конкретної бази даних, яку ви використовуєте. Треба налаштувати і прописати пароль та юзернейм для бази даних, яка використовується на цьому проекті. Нижче наведений приклад

конфігурації та додавання даних до таблиць для використання бази даних PostgreSQL. (Рис.3.4, 3.5):

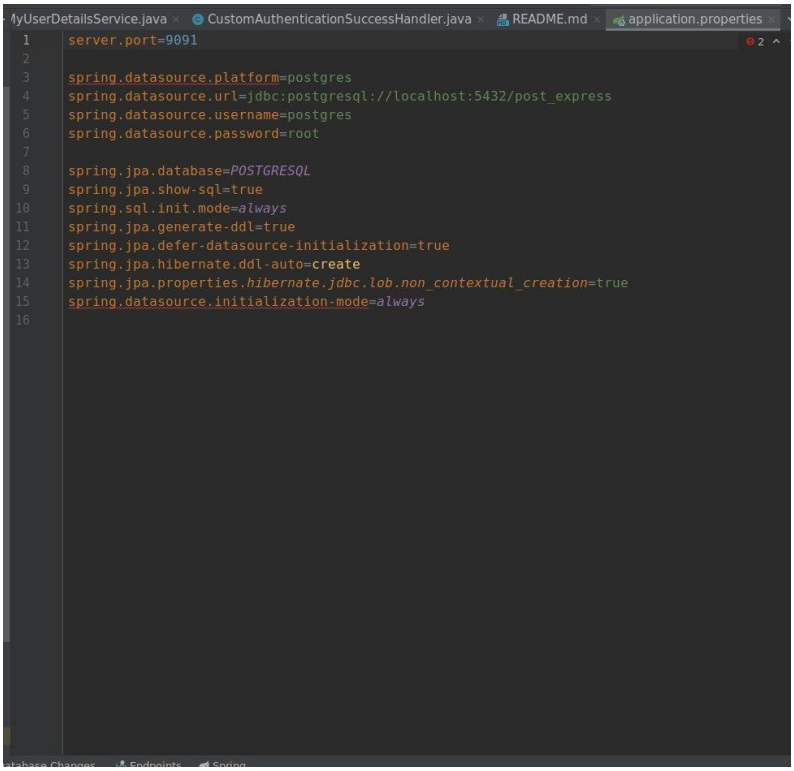


Рисунок 3.4 — Налаштування application.properties для БД [38]

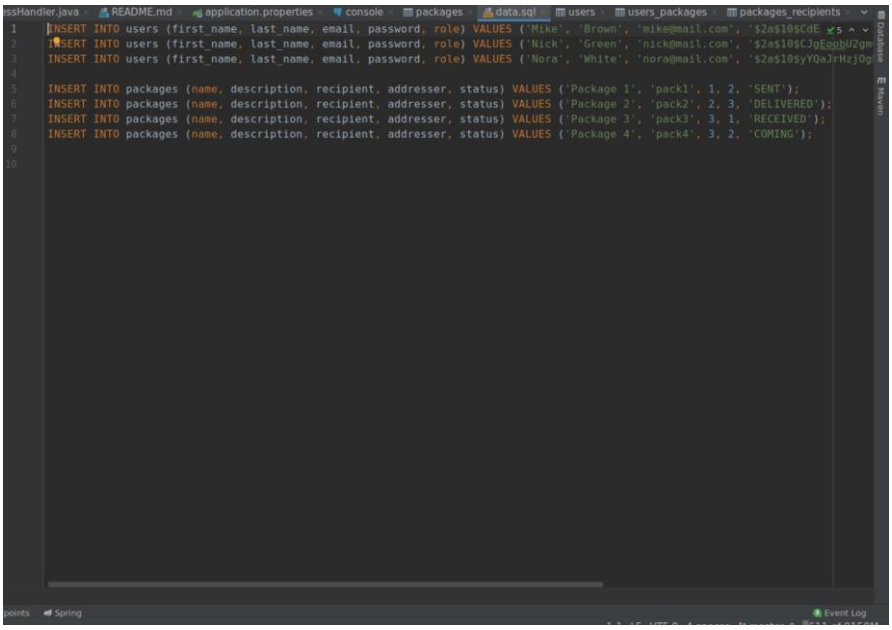
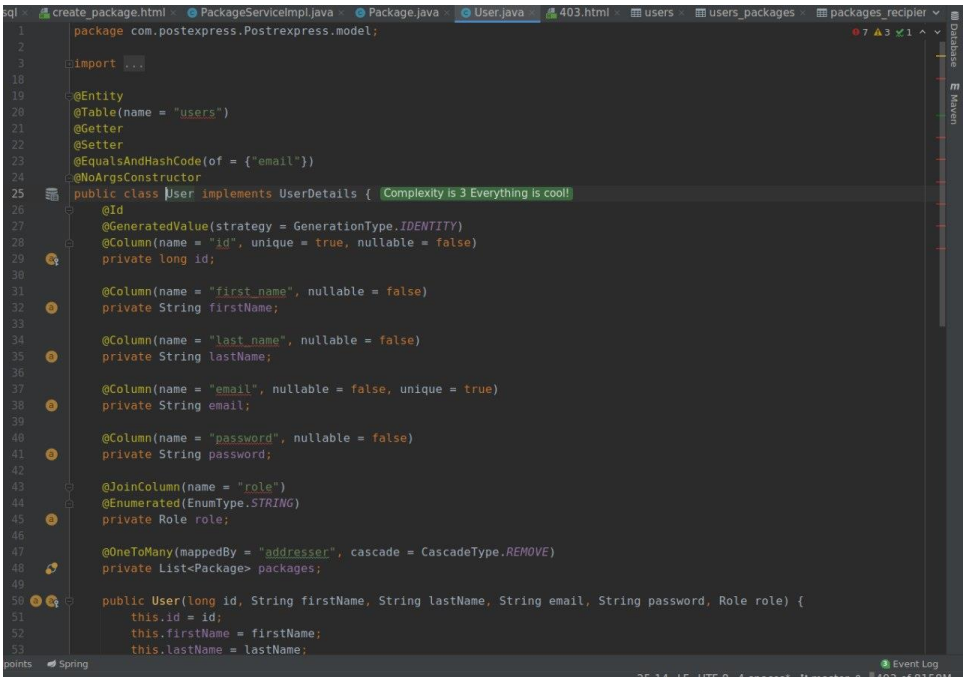


Рисунок 3.5 — Додавання даних до БД [38]

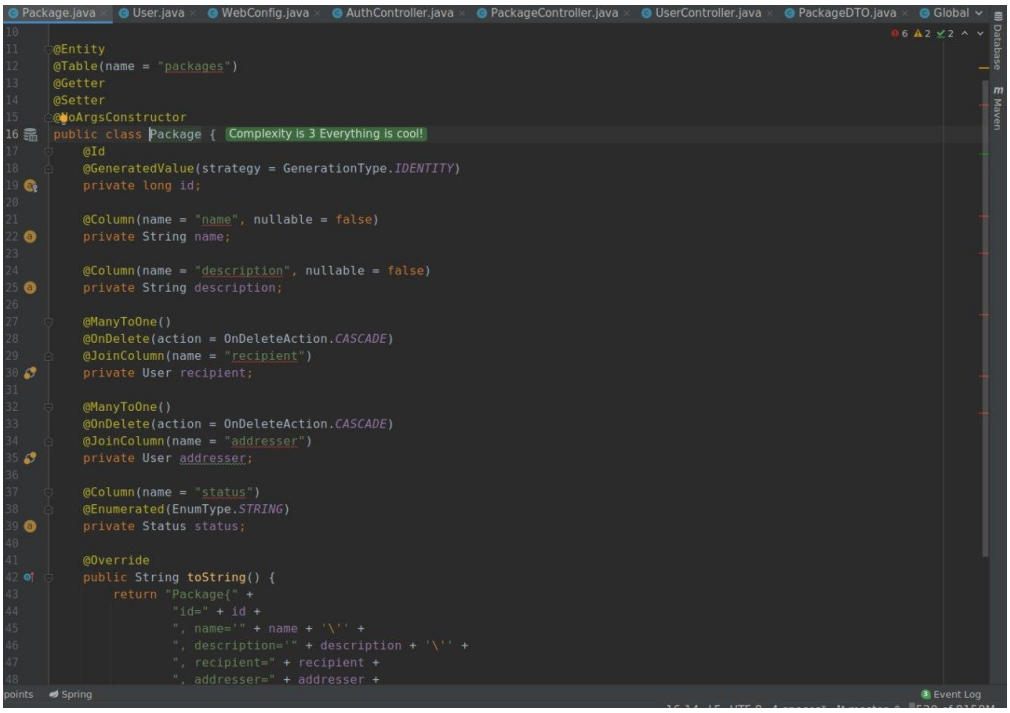
3.7.3 Розробка ключових моделей нашого проекту. Головною частиною у розробці сайту є користувач. Тому для цього я зробив модель користувача з усіма потрібними для функціювання полями (Рис.3.6):



```java
package com.postexpress.Postrexpress.model;

import ...

@Entity
@Table(name = "users")
@Getter
@Setter
@EqualsAndHashCode(of = {"email"})
@NoArgsConstructor
public class User implements UserDetails {  Complexity is 3 Everything is cool!
    @Id
    @GeneratedValue(strategy = GenerationType.IDENTITY)
    @Column(name = "id", unique = true, nullable = false)
    private long id;

    @Column(name = "first_name", nullable = false)
    private String firstName;

    @Column(name = "last_name", nullable = false)
    private String lastName;

    @Column(name = "email", nullable = false, unique = true)
    private String email;

    @Column(name = "password", nullable = false)
    private String password;

    @JoinColumn(name = "role")
    @Enumerated(EnumType.STRING)
    private Role role;

    @OneToMany(mappedBy = "addresser", cascade = CascadeType.REMOVE)
    private List<Package> packages;

    public User(long id, String firstName, String lastName, String email, String password, Role role) {
        this.id = id;
        this.firstName = firstName;
        this.lastName = lastName;
```

Рисунок 3.6 — Модель користувача [38]

Другою важливою за складовою є модель контейнер, яка повинаа мати відправника, отримувача, опис та статус, йде чи пакується, наприклад. (Рис.3.7):



```java
@Entity
@Table(name = "packages")
@Getter
@Setter
@NoArgsConstructor
public class Package {  Complexity is 3 Everything is cool!
    @Id
    @GeneratedValue(strategy = GenerationType.IDENTITY)
    private long id;

    @Column(name = "name", nullable = false)
    private String name;

    @Column(name = "description", nullable = false)
    private String description;

    @ManyToOne()
    @OnDelete(action = OnDeleteAction.CASCADE)
    @JoinColumn(name = "recipient")
    private User recipient;

    @ManyToOne()
    @OnDelete(action = OnDeleteAction.CASCADE)
    @JoinColumn(name = "addresser")
    private User addresser;

    @Column(name = "status")
    @Enumerated(EnumType.STRING)
    private Status status;

    @Override
    public String toString() {
        return "Package{" +
                "id=" + id +
                ", name='" + name + '\'' +
                ", description='" + description + '\'' +
                ", recipient=" + recipient +
                ", addresser=" + addresser +
```

Рисунок 3.7 — Модель контейнера [38]

Також, нам потрібні константи статусу контейнера та ролі користувача. (Рис.3.8, Рис.3.9):

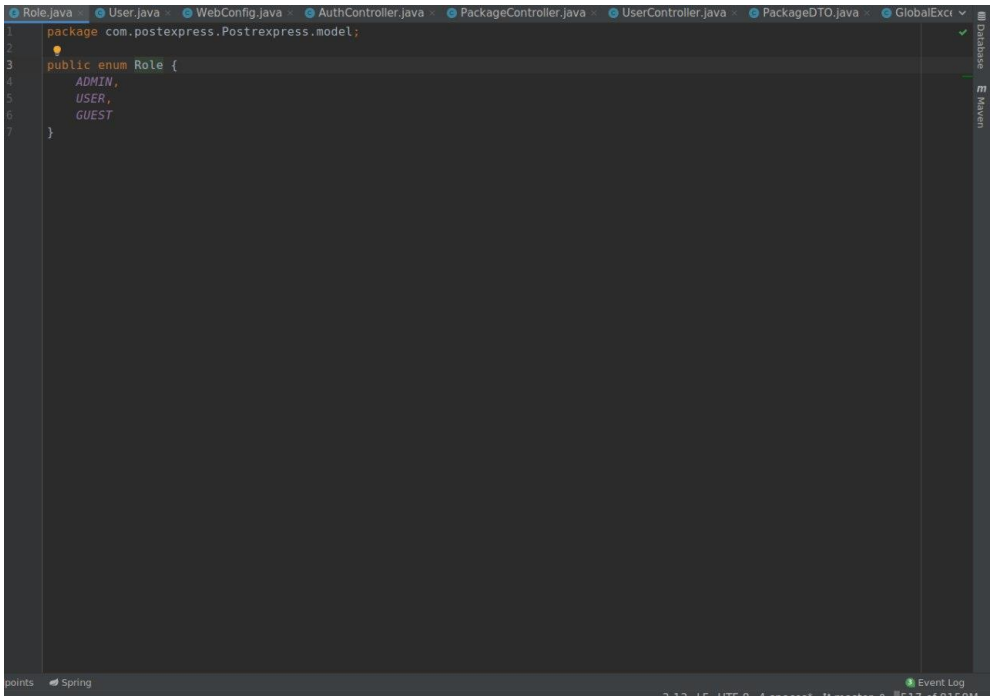


Рисунок 3.8 — Константи ролей [38]

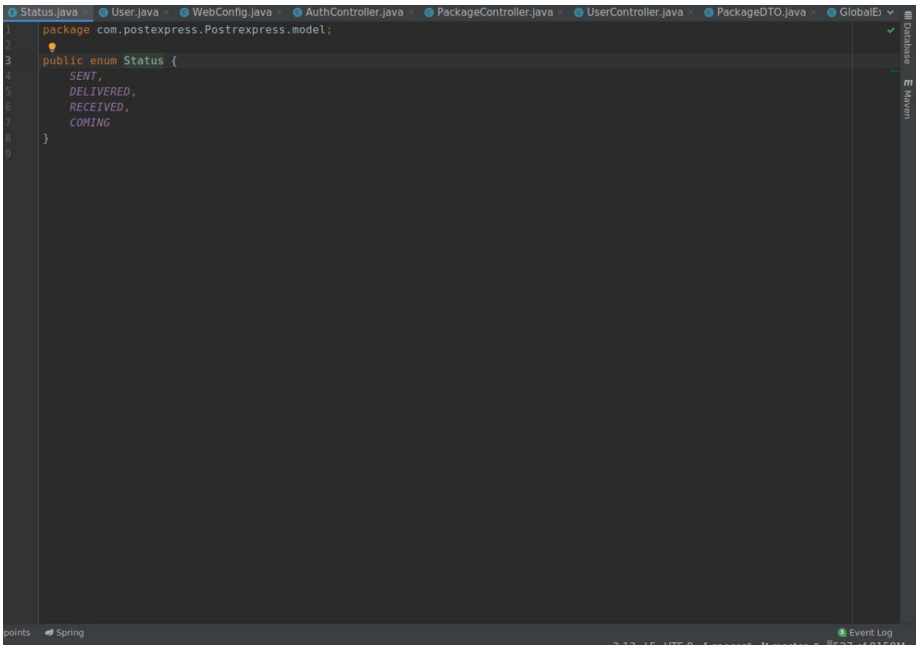


Рисунок 3.9 — Константи статусу [38]

3.7.4 Написання коду нашого проекту. UserRepository.java. Витягування з бази даних потрібних значень. Ця конфігурація відповідає за витягування значень моделі користувача, тобто використовується для виконання операцій бази даних, таких як зберігання, оновлення, видалення та витягування даних. (Рис.3.10):

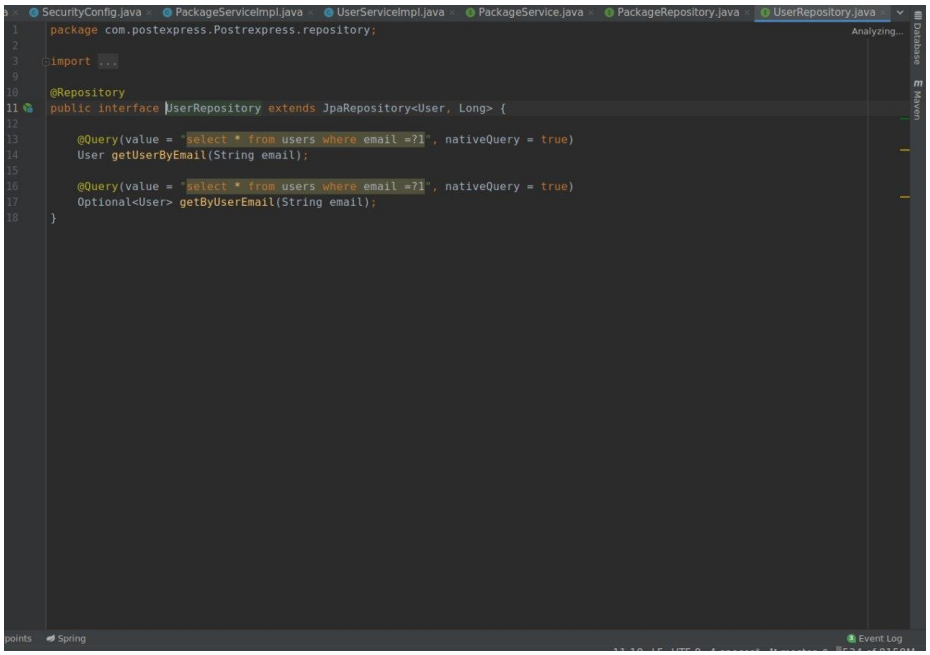


Рисунок 3.10 — Репозиторій UserRepository [38]

PackageRepository.java

Витягування з бази даних потрібних значень (Рис.3.10).

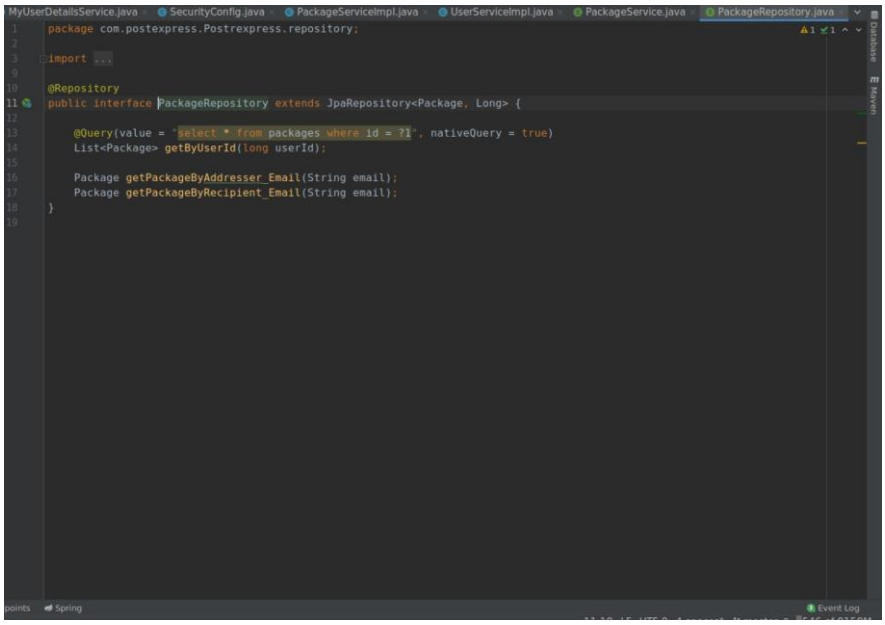


Рисунок 3.10 — Репозиторій PackageRepository [38]

Ця конфігурація відповідає за витягування значень моделі користувача, тобто для витягування та взаємодії з даними моделі "Package" (Рис.3.11):

UserServiceImpl.java

У файлі UserServiceImpl.java, який реалізує бізнес-логіку для користувачів. Цей клас включає в себе методи для обробки операцій з користувачами, які викликають методи UserRepository. (Рис.3.11):

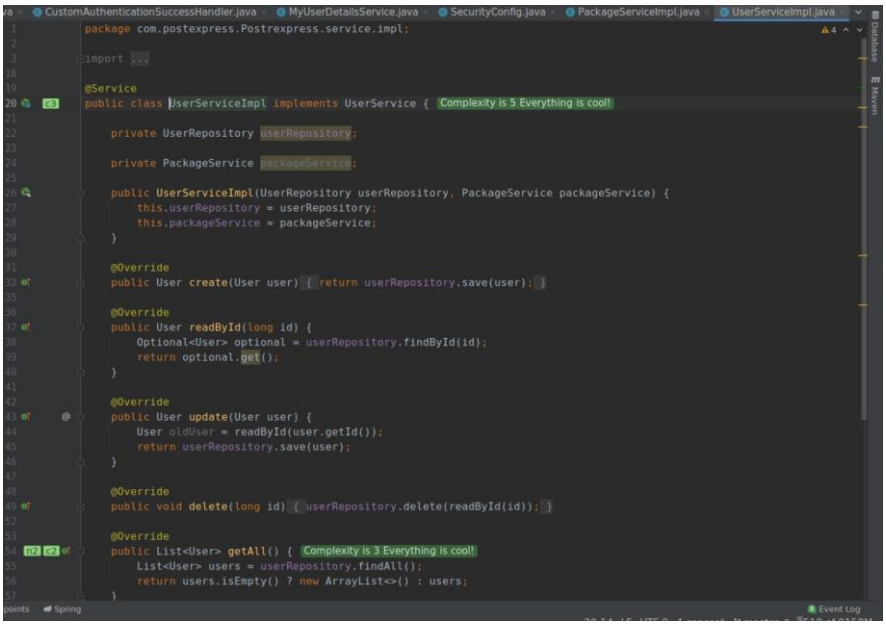


Рисунок 3.11 — Сервіс UserServiceImpl [38]

PackageServiceImpl.java. У файлі PackageServiceImpl.java, який реалізує бізнес-логіку для контейнерів. Цей клас включає в себе методи для обробки операцій з контейнерами, які викликають методи PackageRepository. (Рис.3.12):

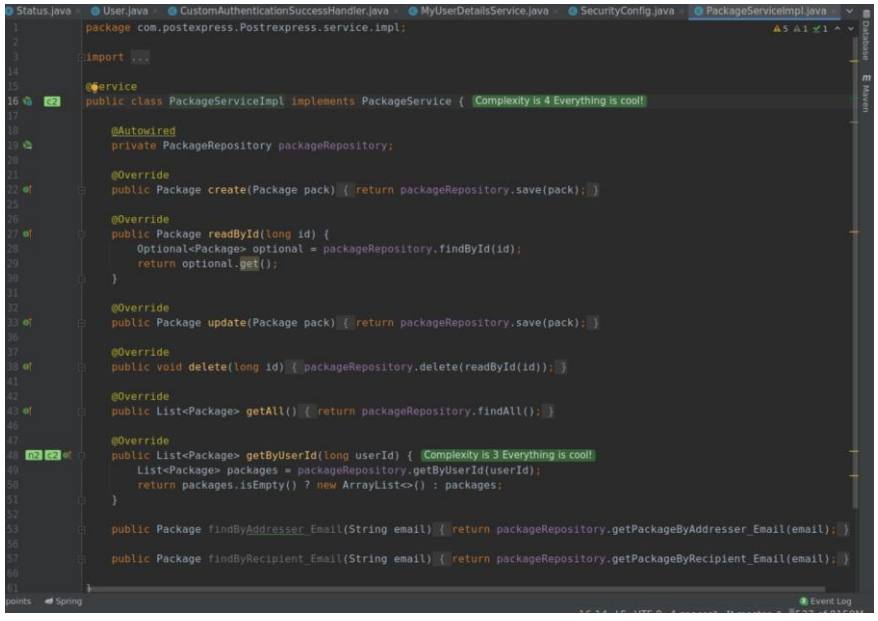


Рисунок 3.12 — Сервіс PackageServiceImpl [38]

GlobalExceptionHandler.java. GlobalExceptionHandler - це клас в Spring, який служить для глобального обробки винятків або помилок в вашому додатку. Він може включати логіку обробки помилок, які виникають на рівні контролерів або сервісів, і надає зручний спосіб централізованої обробки помилок для всього додатку. (Рис.3.13):

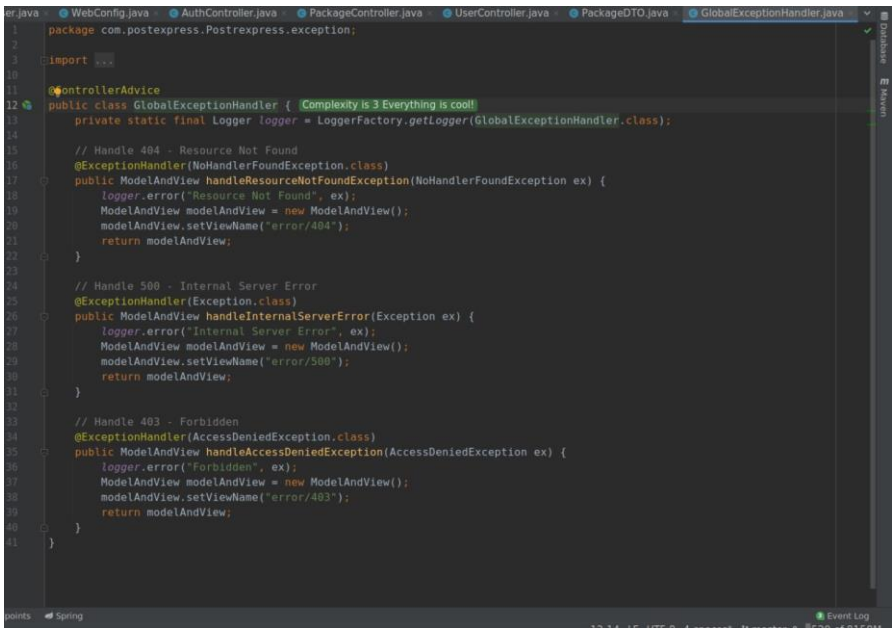


Рисунок 3.13 — Обробник GlobalExceptionHandler [38]

create_package.html. create_package.html у контексті Thymeleaf виглядатиме як файл шаблону, що використовується для відображення форми створення нового контейнера. (Рис.3.14):

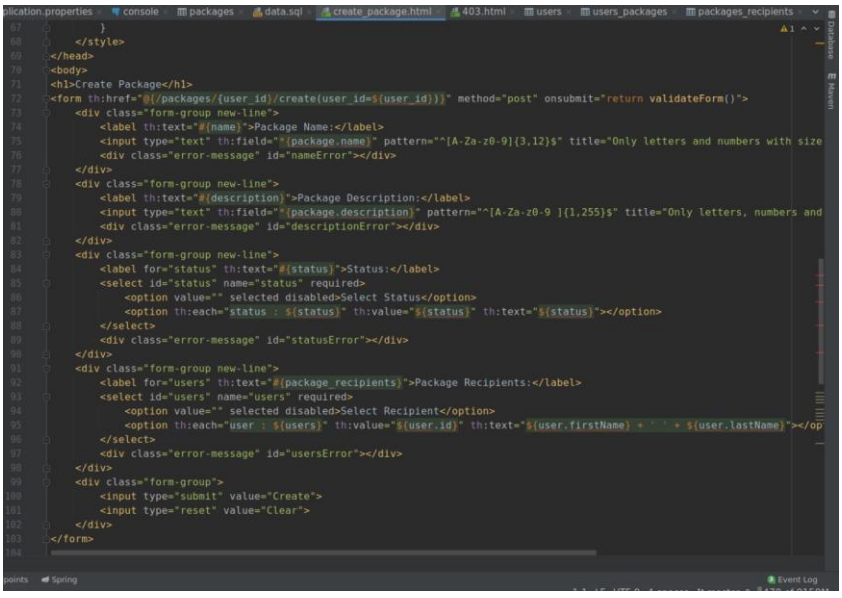


Рисунок 3.14 — Шаблон створення контейнера [38]

home.html. home.html у контексті Thymeleaf може виглядати як сторінка, яка відображає домашню сторінку нашого додатку. (Рис.3.15):

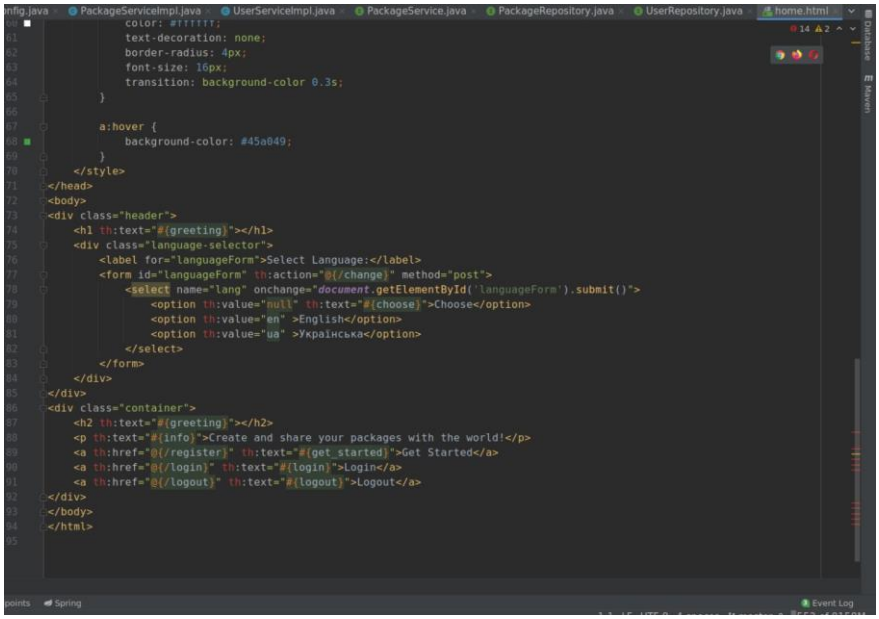


Рисунок 3.15 — Шаблон домашньої сторінки [38]

login.html

Файл login.html у контексті Thymeleaf використовується для відображення сторінки входу (login page). (Рис.2.15):

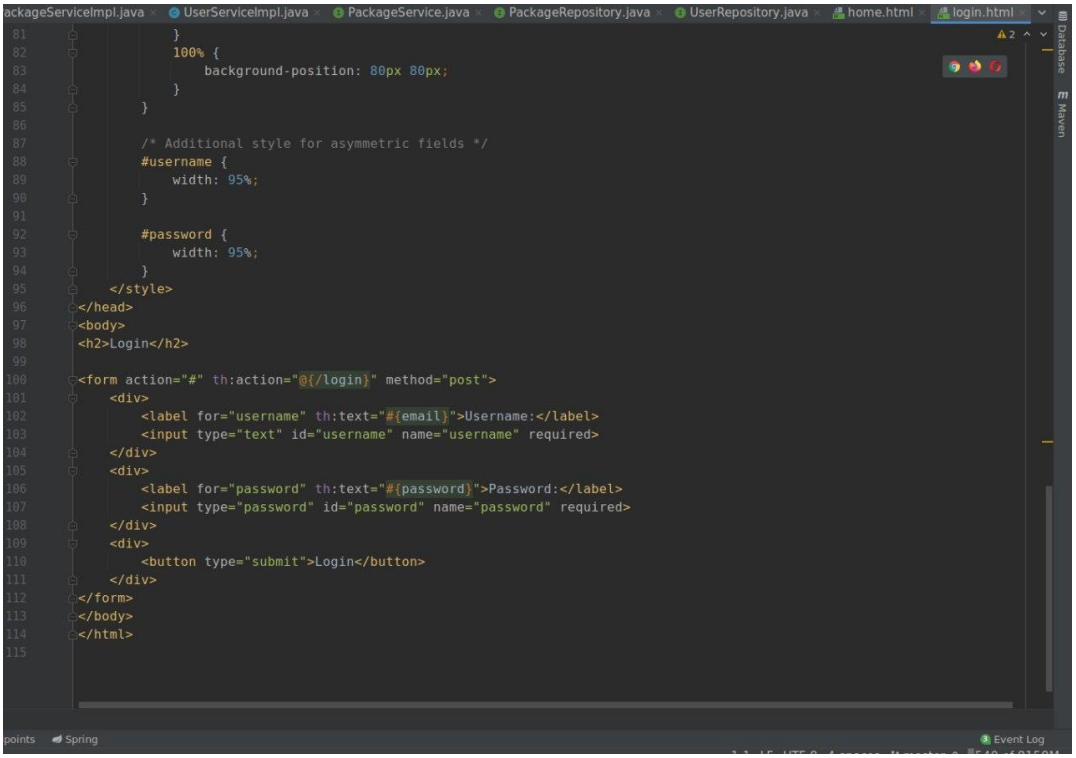
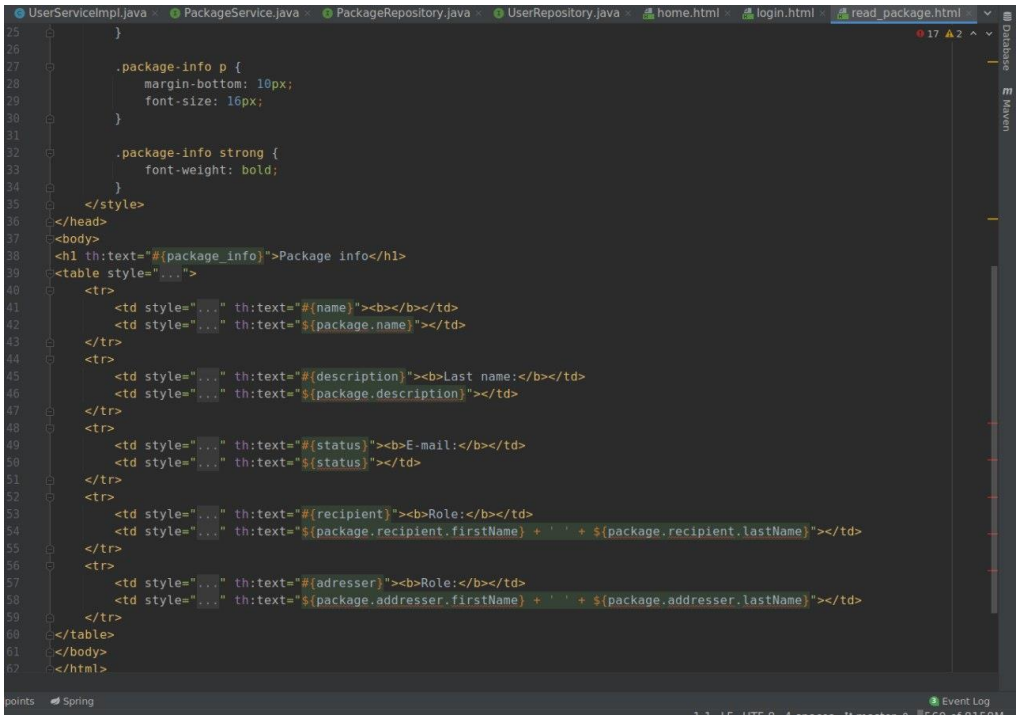


Рисунок 3.16 — Шаблон сторінки входу [38]

read_package.html. read_package.html у контексті Thymeleaf використовується для відображення інформації про конкретний контейнер. (Рис.3.17):




```
        }

        .package-info p {
            margin-bottom: 10px;
            font-size: 16px;
        }

        .package-info strong {
            font-weight: bold;
        }
    </style>
</head>
<body>
 <h1 th:text="#{package_info}">Package info</h1>
<table style="...">
    <tr>
        <td style="..." th:text="#{name}"><b></b></td>
        <td style="..." th:text="${package.name}"></td>
    </tr>
    <tr>
        <td style="..." th:text="#{description}"><b>Last name:</b></td>
        <td style="..." th:text="${package.description}"></td>
    </tr>
    <tr>
        <td style="..." th:text="#{status}"><b>E-mail:</b></td>
        <td style="..." th:text="${status}"></td>
    </tr>
    <tr>
        <td style="..." th:text="#{recipient}"><b>Role:</b></td>
        <td style="..." th:text="${package.recipient.firstName} + ' ' + ${package.recipient.lastName}"></td>
    </tr>
    <tr>
        <td style="..." th:text="#{adresser}"><b>Role:</b></td>
        <td style="..." th:text="${package.addresser.firstName} + ' ' + ${package.addresser.lastName}"></td>
    </tr>
</table>
</body>
</html>
```

Рисунок 3.17 — Шаблон сторінки інформації про контейнер [38]

register.html. register.html у контексті Thymeleaf використовується для відображення сторінки реєстрації користувача. (Рис.3.18):

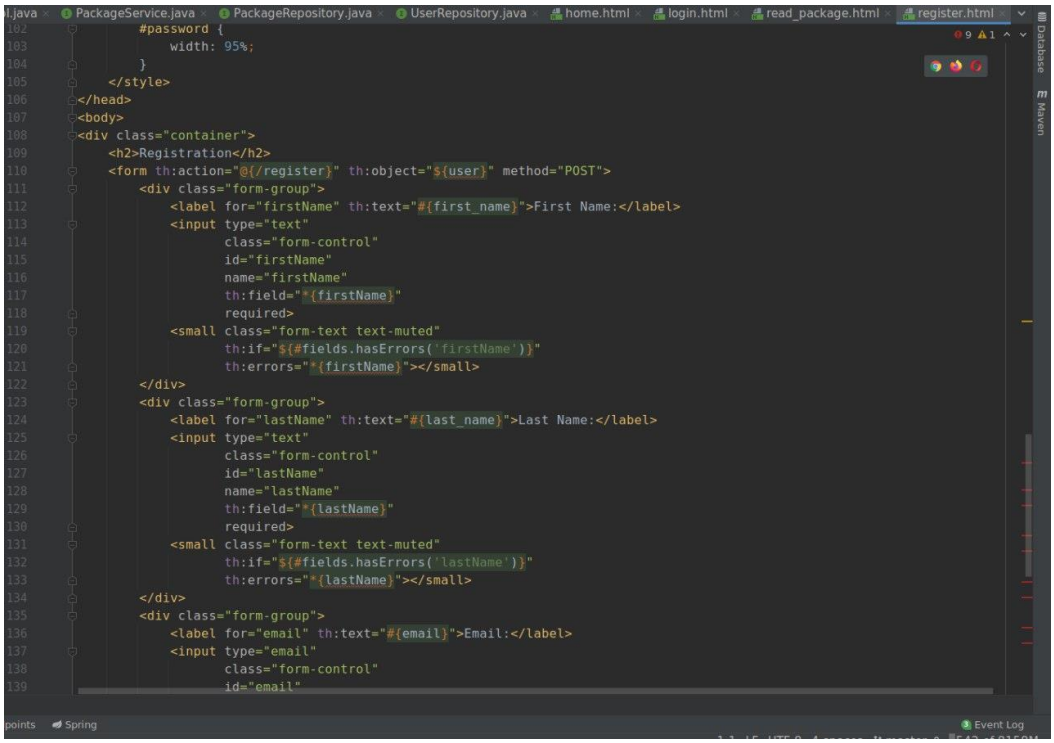


Рисунок 3.18 — Шаблон сторінки реєстрації [38]

update_user.html. update_user.html у контексті Thymeleaf використовується для відображення сторінки оновлення інформації про користувача. (Рис.3.19):

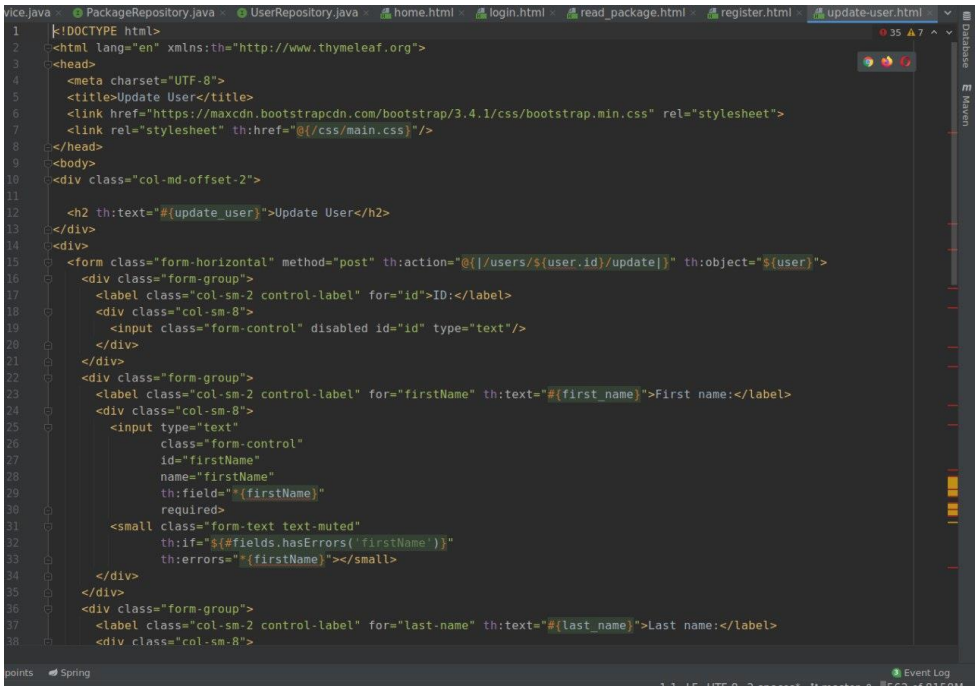


Рисунок 3.19 — Шаблон сторінки оновлення користувача [38]

update_package.html. update_package.html у контексті Thymeleaf використовується для відображення сторінки оновлення інформації про контейнер. (Рис.3.20):

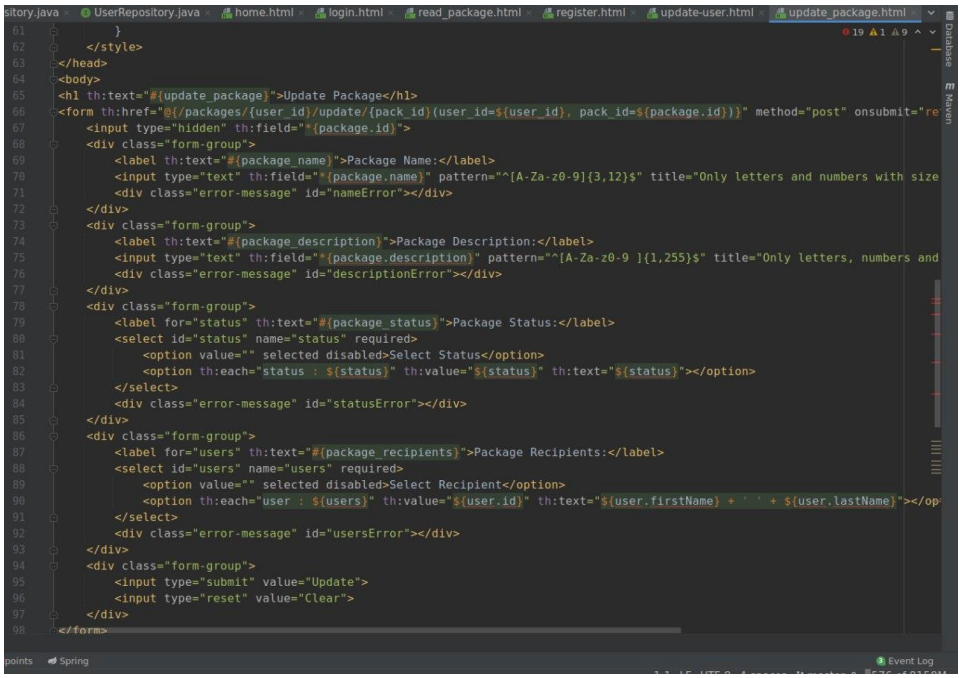


Рисунок 2.19 — Шаблон сторінки оновлення контейнера [38]

user_info.html. user_info.html у контексті Thymeleaf використовується для відображення інформації про користувача. (Рис.3.21):

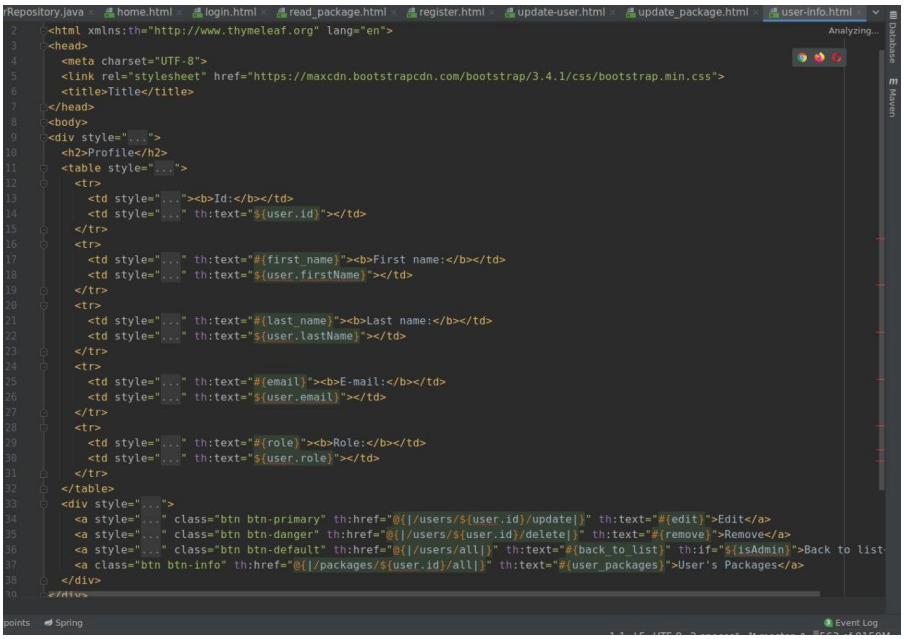


Рисунок 3.21 — Шаблон сторінки інформації про користувача [38]

user_packages.html. user_packages.html у контексті Thymeleaf виглядає як сторінка, що відображає пакунки, пов'язані з певним користувачем. (Рис.3.22):

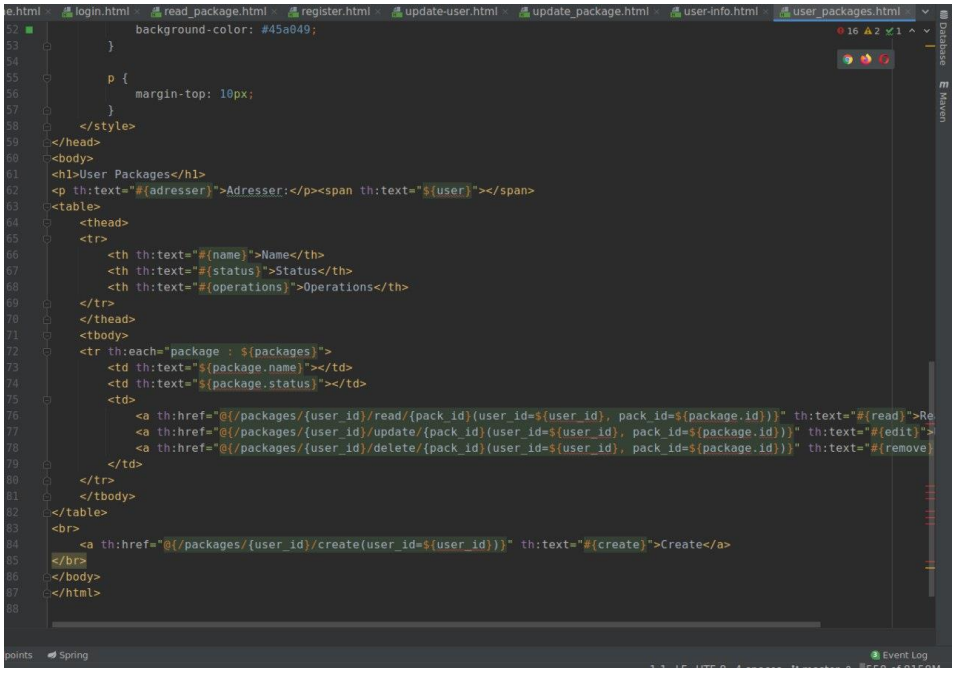


Рисунок 3.22 — Шаблон сторінки інформації про контейнери користувача [38]

users_list.html. users_list.html у контексті Thymeleaf використовується для відображення списку користувачів, у першу чергу доступний тільки для адмінів веб-сайту. (Рис.3.23):

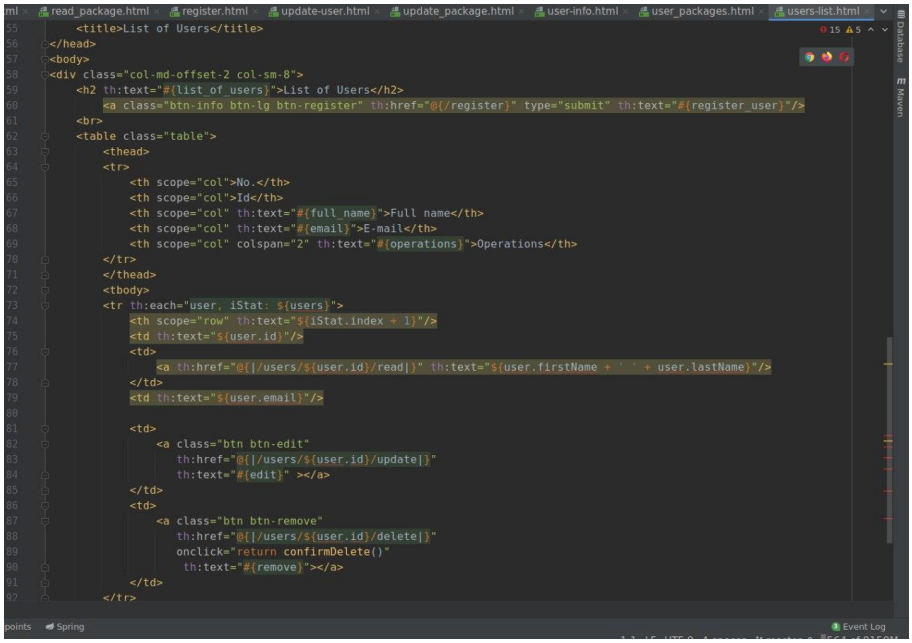


Рисунок 3.23 — Шаблон сторінки інформації про користувачів [38]

README.md. README-файл (readme.md) у нашому проекті служить для надання короткої, зрозумілої інформації про ваш проект. Він включає інформацію про зареєстрованих юзерів (адміни та звичайні), залежності, які були використані, та показано візуально – як виглядає веб-сайт. (Рис.3.24):

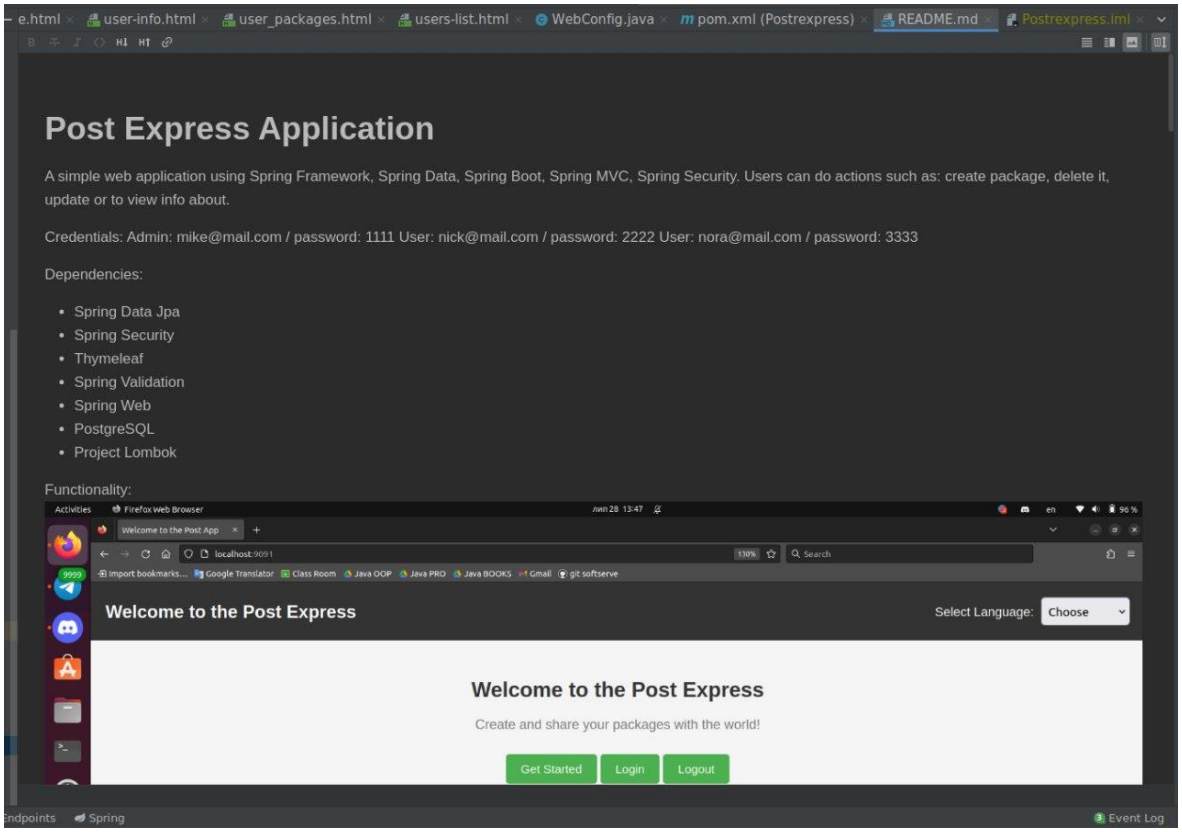


Рисунок 3.24 — Файл README [38]

3.7.5 Написання коду для автентифікації та авторизації користувача. Одним з найпростіших і найпоширеніших методів автентифікації є базова автентифікація, яка передбачає надсилання облікових даних користувача в HTTP-заголовку кожного запиту. Потім веб-сервер звіряє облікові дані з базою даних або файлом і відповідає або кодом успіху, або кодом помилки. Базова автентифікація проста в реалізації і сумісна з більшістю браузерів і клієнтів, але вона має деякі недоліки, наприклад, виставляє облікові дані у вигляді простого тексту, вимагає від користувача вводити їх щоразу, а також не підтримує вихід з системи або управління сесіями.

UserController.java

UserController.java - це клас контролера веб-додатка, який відповідає за обробку запитів, пов'язаних з операціями, що стосуються користувачів. Такі операції можуть включати отримання інформації про користувача, створення нового користувача, оновлення інформації, видалення користувача та інші. (Рис.3.25):

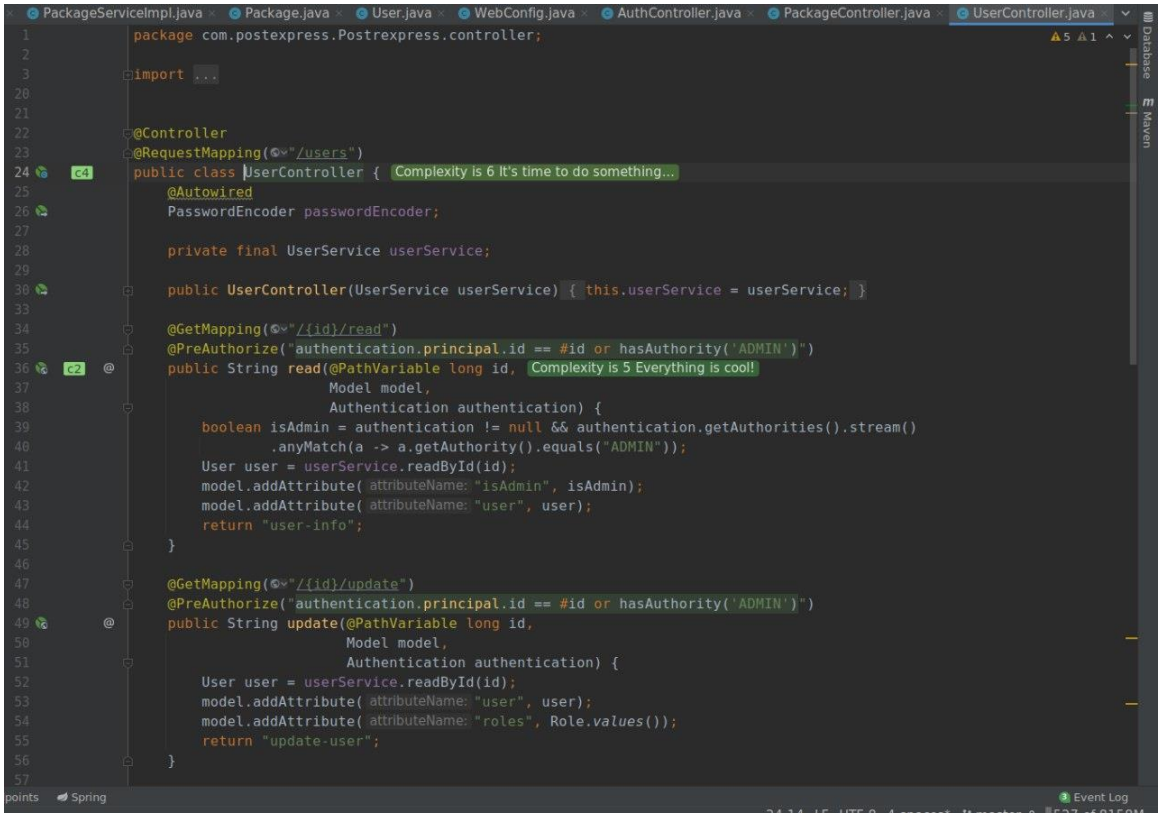


Рисунок 3.25 — Контролер UserController [38]

CustomAuthenticationSuccessHandler.java

CustomAuthenticationSuccessHandler - це клас, який використовується для налаштування власної поведінки після успішної аутентифікації користувача. (Рис 3.26):

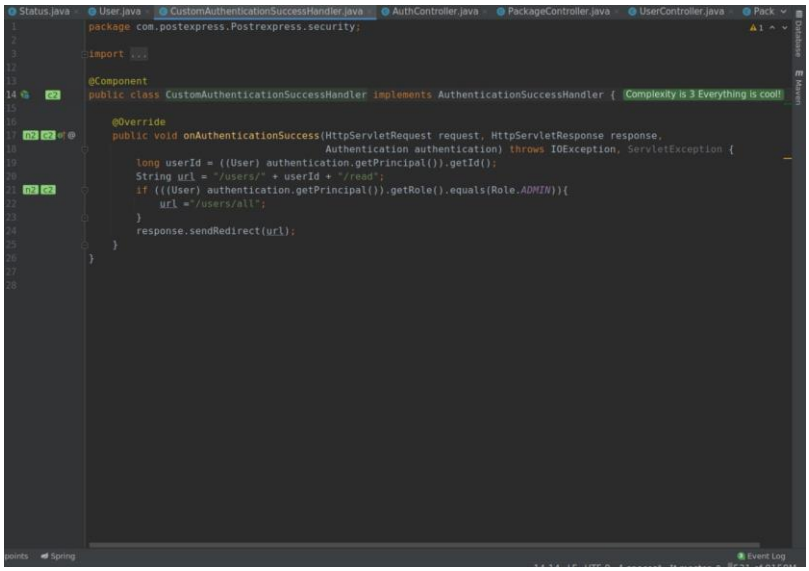


Рисунок 3.26 — Менеджер CustomAuthenticationSuccessHandler [38]

AuthController.java

AuthController.java є класом, який відповідає за обробку запитів, пов'язаних з аутентифікацією (authentication) і авторизацією (authorization) у нашому веб-додатку. Зазвичай це включає в себе обробку входу в систему, реєстрації користувачів, виходу з системи та інших подій, пов'язаних із безпекою. (Рис.3.27):

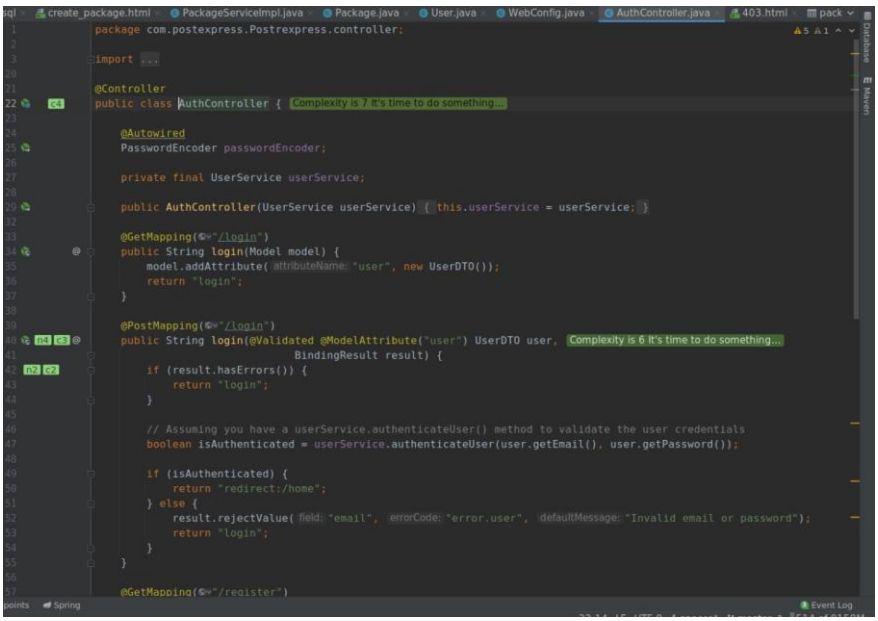


Рисунок 3.27 — Контролер AuthController [38]

PackageController.java

PackageController.java є класом контролера веб-додатка, який відповідає за обробку запитів, пов'язаних з операціями над контейнерами чи іншими об'єктами, які представляють контейнери. (Рис.3.28):

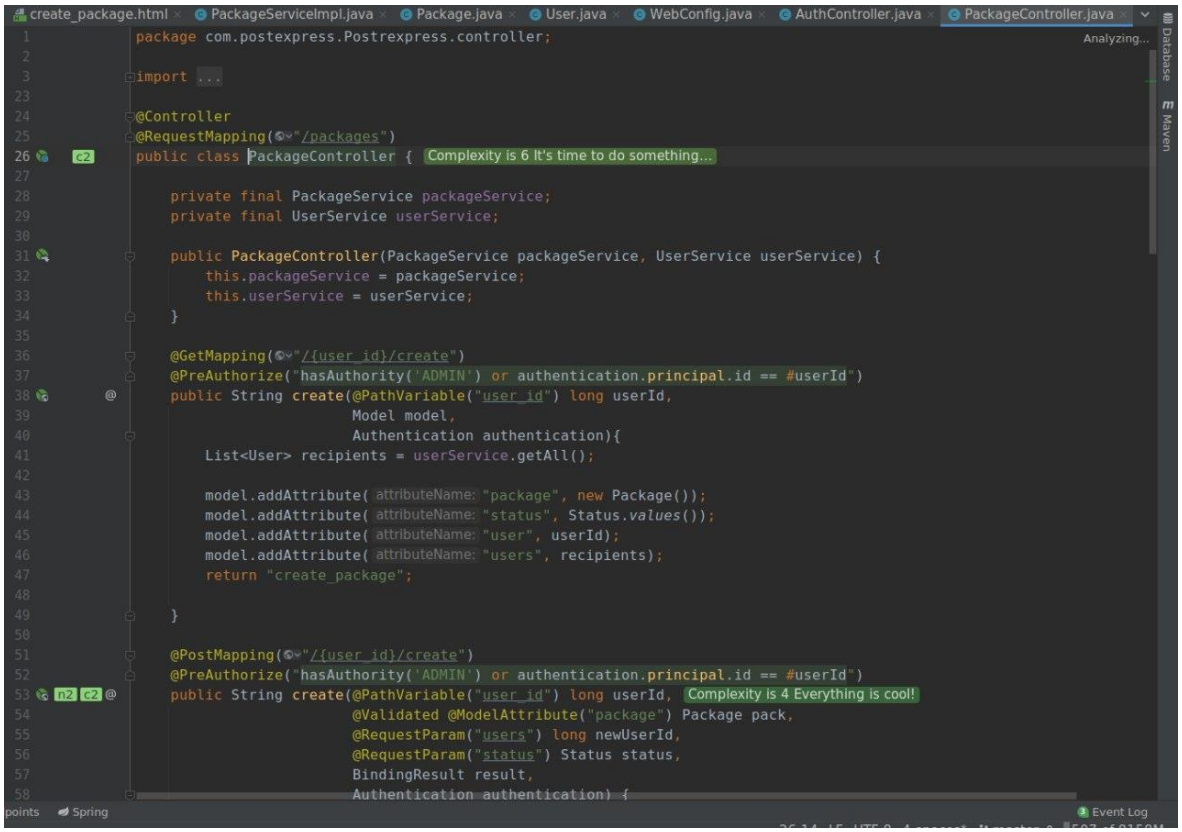


Рисунок 3.28 — Контролер PackageController [38]

MyUserDetailsService.java

У Spring Security UserDetails - це інтерфейс, який надає необхідну інформацію про користувача для системи безпеки. Він містить такі дані, як ім'я користувача, пароль і надані повноваження, а також інформацію про стан облікового запису. Сюди входить інформація про те, чи обліковий запис увімкнено, заблоковано, термін дії облікових даних закінчився або термін дії облікового запису закінчився. Цей інтерфейс зазвичай корисний, коли вам потрібно завантажити специфічні для користувача дані під час процесу автентифікації.

MyUserDetailsService - це сервіс користувачів, який реалізує інтерфейс UserDetailsService з Spring Security. Його основним завданням є завантаження даних користувача з бази даних та створення об'єкта UserDetails, який

використовується Spring Security для подальшої обробки аутентифікації та авторизації. (Рис.3.29):

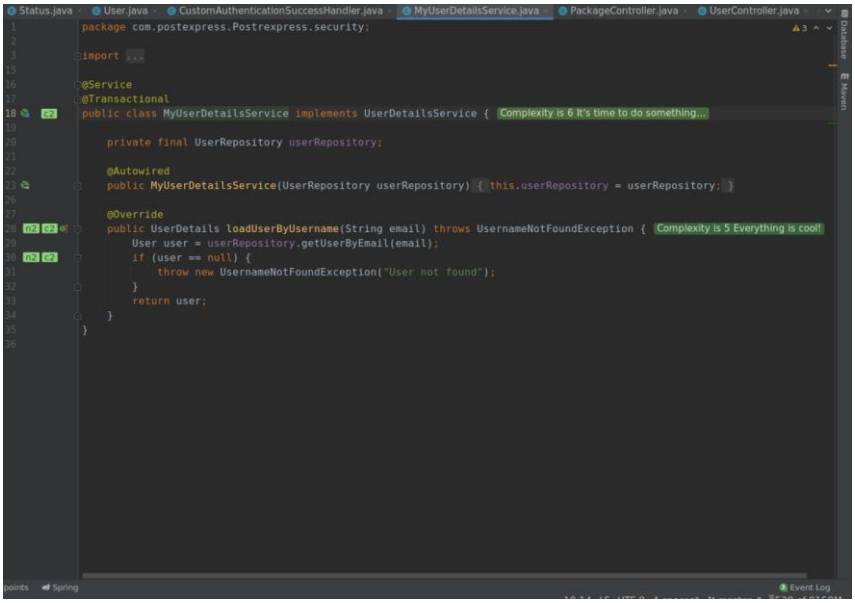


Рисунок 3.29 — Сервіс MyUserDetailsService [38]

SecurityConfig.java

Основна ідея полягає в тому, що ви можете створити свій власний клас, який розширює WebSecurityConfigurerAdapter, і визначити свої власні налаштування безпеки в методах цього класу. Таким чином, ви можете керувати тим, як Spring Security обробляє аутентифікацію, авторизацію та інші аспекти безпеки вашого додатку. (Рис.3.30):

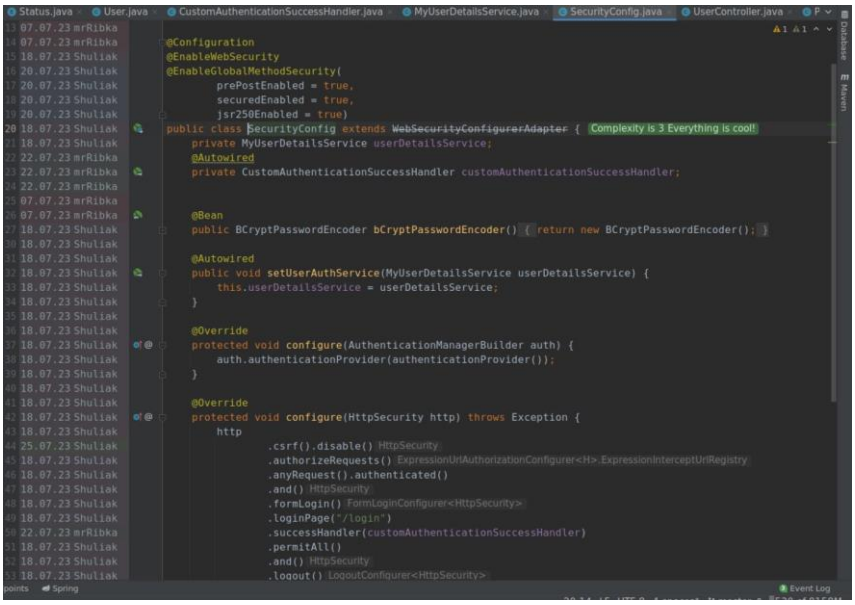


Рисунок 3.31 — Адаптер SecurityConfig [38]

WebConfig.java

Клас WebMvcConfigurerAdapter, який раніше був частиною Spring Framework, був використаний для налаштування параметрів конфігурації Spring MVC. Тому для конфігурації ми можемо створити власний клас та розширити його функціонал. (Рис.3.31):

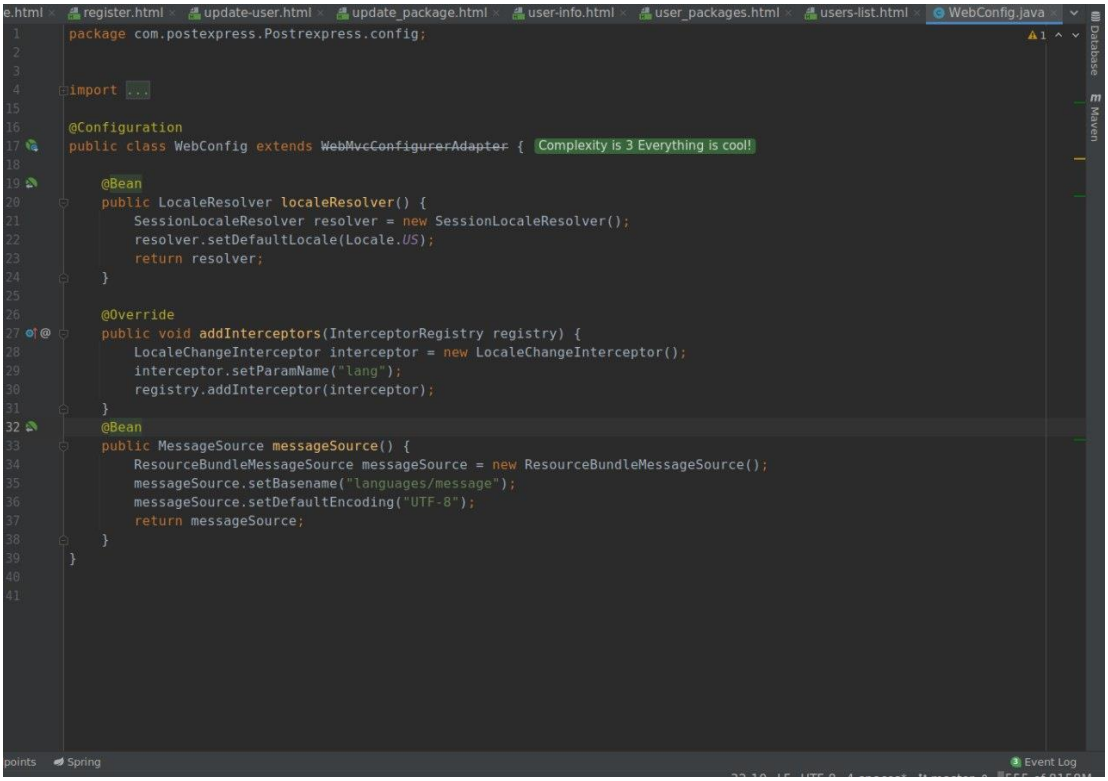


Рисунок 3.31 — Адаптер WebConfig [38]

3.7.6 Візуальне представлення веб-додатку

1. Домашня сторінка (Рис.3.32)

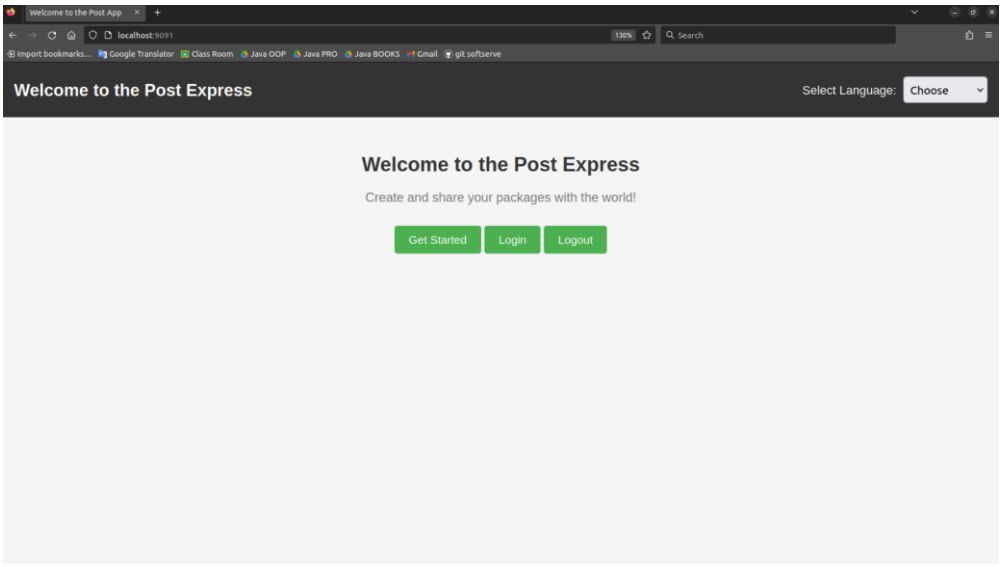


Рисунок 3.32 — Домашня сторінка [38]

2. Сторінка входу (Рис.3.33)

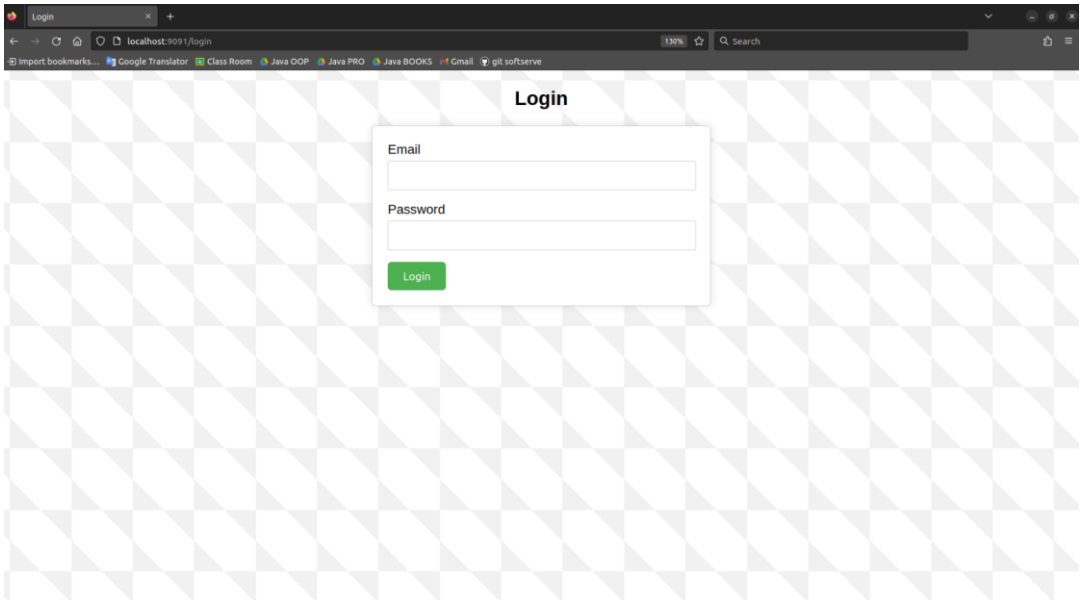


Рисунок 3.33 — Сторінка входу [38]

3. Сторінка реєстрації (Рис.3.34)

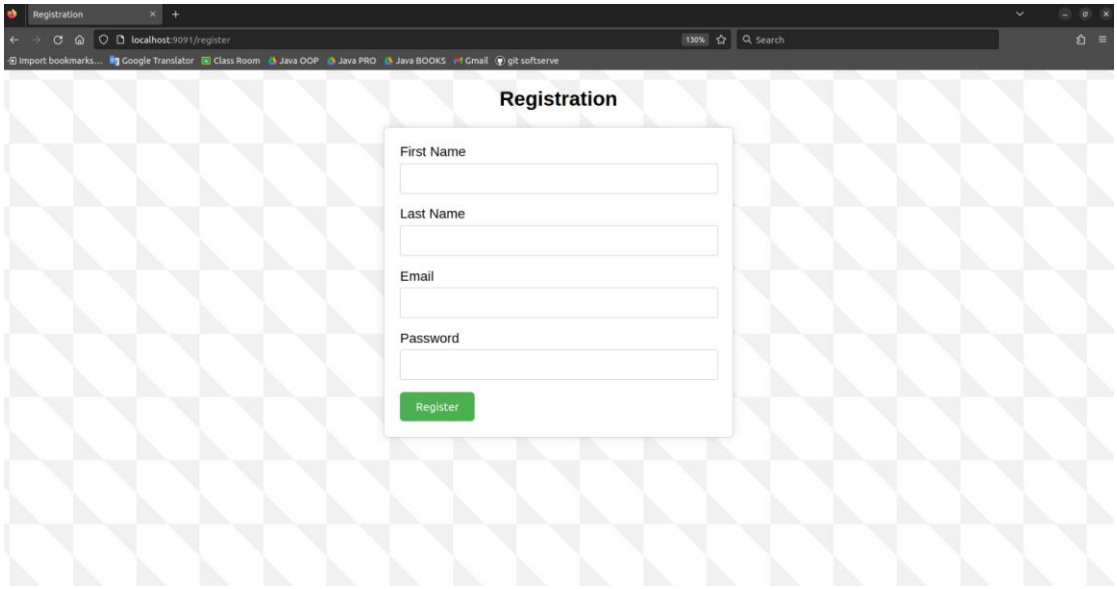


Рисунок 3.34 — Сторінка реєстрації [38]

4.Профіль(Рис.3.35)

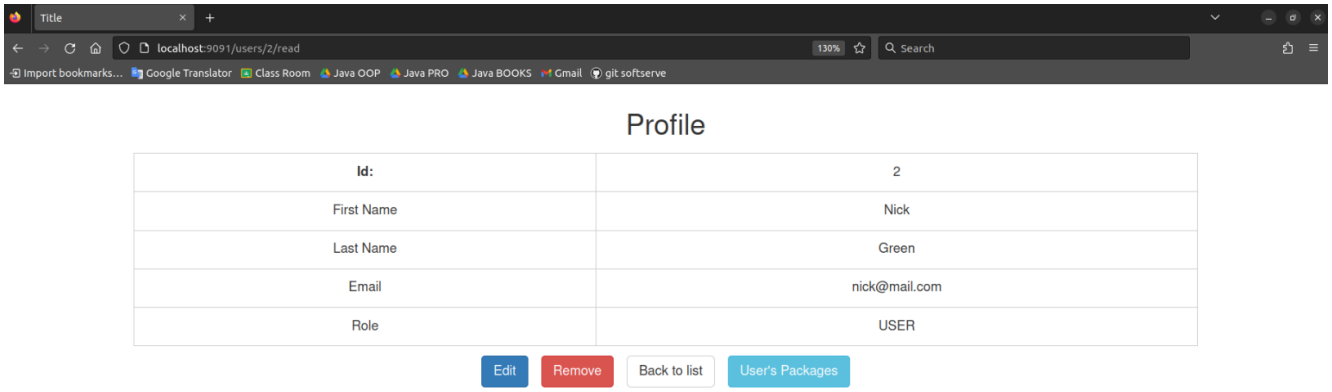


Рисунок 3.35 — Профіль [38]

5. Сторінка створення контейнеру(Рис.3.36)

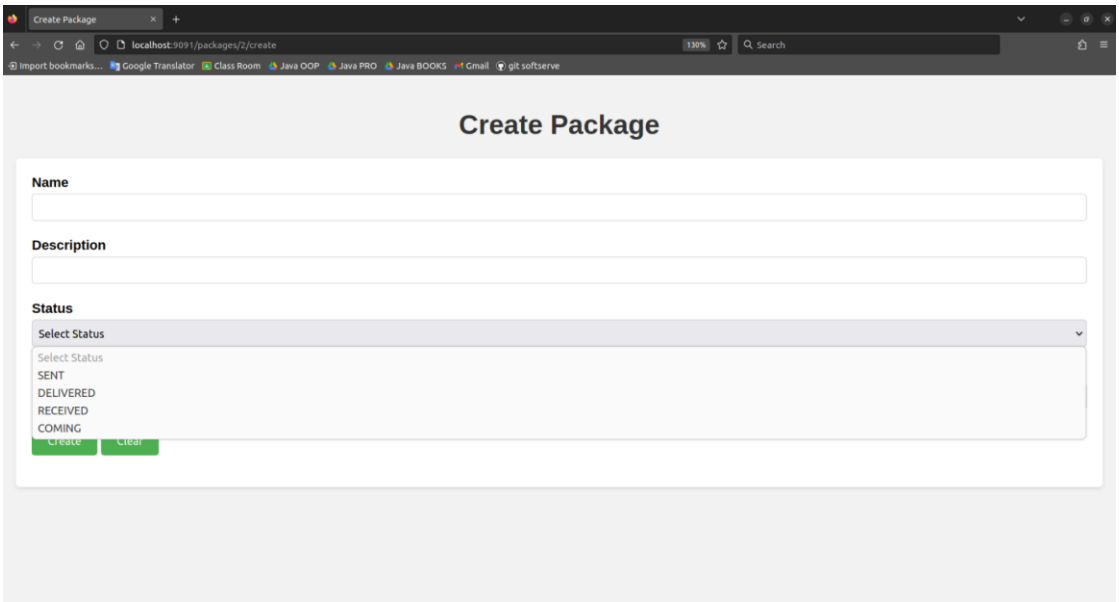


Рисунок 3.36 — Сторінка створення контейнеру [38]

6. Список всіх користувачів(Рис.3.37)

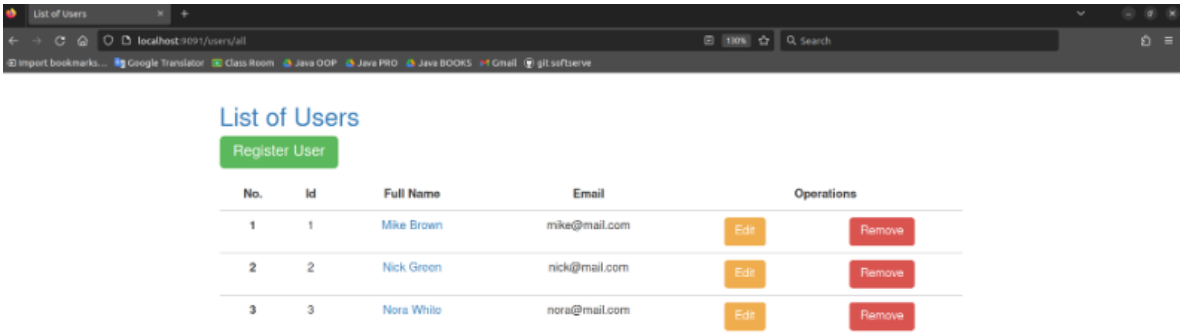


Рисунок 3.37 — Список всіх користувачів [38]

ВИСНОВКИ

Під час виконання атестаційної магістерської роботи була розглянута актуальна проблема створення логістичного додатку для мобільних працівників, диспетчерів, водіїв і кур'єрів, які займаються доставкою товарів роздрібним продавцям або клієнтам.

У процесі дослідження визначено предмет та об'єкт дослідження, проведений аналіз методів і принципів побудови систем управління логістикою. Також була розроблена система управління логістикою, строго виконуючи план розробки програмного забезпечення.

Аналізуючи недоліки та проблеми у процесі розробки веб-додатку, було поставлено завдання щодо дослідження та запропонована ефективна розробка, заснована на фреймворку Spring з підтримкою мови програмування Java.

Це дозволило досягти поставлених мет ці:

1. Підвищення ефективності розробки моделей.
2. Збільшення швидкості веб-додатку.
3. Додана аутентифікація та авторизація для користувачів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Електронна комерція// [Електронний ресурс] Режим доступу до ресурсу: https://uk.cqlife.net/e-commerce#google_vignette(дата звернення: 20.12.2023).
2. Особливості електронної комерції та стан її розвитку в сучасних економічних умовах України// [Електронний ресурс] Режим доступу до ресурсу: http://www.economy.nayka.com.ua/pdf/12_2018/76.pdf(дата звернення: 20.12.2023).
3. АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЕЛЕКТРОННОЇ КОМЕРЦІЇ В УКРАЇНІ // [Електронний ресурс] Режим доступу до ресурсу: http://www.lsej.org.ua/9_2020/71.pdf(дата звернення: 20.12.2023).
4. Ключові проблеми кібербезпеки в логістиці та їх рішення// [Електронний ресурс] Режим доступу до ресурсу: https://wezom.com.ua/ua/blog/klyuchovi-problemi-kiberbezpeki-v-logistitsi-ta-yih-rishennya(дата звернення: 20.12.2023).
5. Fourth-party logistics (4PL): Simplified Definition// [Електронний ресурс] Режим доступу до ресурсу: https://www.clickpost.ai/resources/glossary/4pl-fourth-party-logistics. (дата звернення: 20.12.2023).
6. ТОП 10 загроз кібербезпеці бізнесу у 2023 році// [Електронний ресурс] Режим доступу до ресурсу: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023(дата звернення: 20.12.2023).
7. Fourth-Party Logistics (4PL) // [Електронний ресурс] Режим доступу до ресурсу: https://goodlogisticsgroup.com/4pl/ (дата звернення: 20.12.2023).
8. 4PL Logistics: the next level of supply chain management// [Електронний ресурс] Режим доступу до ресурсу: https://www.blog.shippypro.com/en/4pl (дата звернення: 20.12.2023).
9. Як логістичній галузі відповісти на нові виклики кібербезпеки // [Електронний ресурс] Режим доступу до ресурсу:

https://cfts.org.ua/blogs/yak_logistichniy_galuzi_vidpovisti_na_novi_vikliki_kiberbezpeki_654

10. Захист даних у онлайн-сервісі "Мій Дім Online": Пріоритет безпеки та конфіденційності // [Електронний ресурс] Режим доступу до ресурсу: https://miydimonline.com.ua/uk/blog/zahist-danih-u-onlajn-servisi-mij-dim-online-prioritet-bezpeki-ta-konfidencijnosti(дата звернення: 20.12.2023).
11. Mind Network: розширює можливості забезпечення безпеки та конфіденційності даних в епоху Web3// [Електронний ресурс] Режим доступу до ресурсу: https://medium.com/@nick_rotenberg/mind-network (дата звернення: 20.12.2023).
12. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест/ відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– №10 (жовтень) . – 320 с. // [Електронний ресурс] Режим доступу до ресурсу: https://ippi.org.ua/sites/default/files/2023-10_0.pdf(дата звернення: 20.12.2023).
13. 4 стратегії цифрового маркетингу для збільшення продажів в електронній комерції. // [Електронний ресурс] Режим доступу до ресурсу: https://www.ranktracker.com/uk/blog/4-digital-marketing-strategies-to-boost-your-e-commerce-sales/(дата звернення: 20.12.2023).
14. Як виконувати замовлення для транскордонних продавців електронної комерції? // [Електронний ресурс] Режим доступу до ресурсу: https://leelinesourcing.com/uk/how-to-fulfill-orders-for-cross-border-e-commerce-sellers/(дата звернення: 20.12.2023).
15. eCommerce Shipping: The Best Strategies for eCommerce Businesses // [Електронний ресурс] Режим доступу до ресурсу: https://flowium.com/blog/ecommerce-shipping/#section0 (дата звернення: 20.12.2023).

16. ЯК ЗНАЙТИ ПОТЕНЦІЙНИХ КЛІЄНТІВ // [Електронний ресурс] Режим доступу до ресурсу: https://uk.cathedralcollege.org/encontrar-clientes-potenciales-929 (дата звернення: 20.12.2023).
17. Planning for networking communications [Electronic resource]. – URL: https://www.ibm.com/docs/en/power5?topic=planning-networking-communications (дата звернення: 20.12.2023).
18. База даних [Електронний ресурс] // Wikipedia. – 31 січня 2023. – Режим доступу до ресурсу: http://surl.li/bqulg (дата звернення: 20.12.2023).
19. Managing data confidentiality // [Електронний ресурс] Режим доступу до ресурсу: https://www1.udel.edu/security/data/confidentiality.html (дата звернення: 20.12.2023).
20. What is Data Confidentiality? // [Електронний ресурс] Режим доступу до ресурсу: https://www.secoda.co/glossary/data-confidentiality (дата звернення: 20.12.2023).
21. What is Cyber Security? // [Електронний ресурс] Режим доступу до ресурсу: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security (дата звернення: 20.12.2023).
22. 10 Data Security Best Practices: Simple Methods to Protect Your Data Origin: // [Електронний ресурс] Режим доступу до ресурсу: https://www.ekransystem.com/en/blog/datasecurity-best-practices (дата звернення: 20.12.2023).
23. 10 найкращих блогів електронної комерції, на які варто стежити у 2022 році // [Електронний ресурс] Режим доступу до ресурсу: https://themewp.inform.click/uk/10-najkrashhih-blogiv-elektronnoi-komercii-na-jaki-varto-stezhiti-u-2022-roci/ (дата звернення: 20.12.2023)
24. Порівняння Shopify та Etsy 2023 | Який з них найкращий для вас? // [Електронний ресурс] Режим доступу до ресурсу: https://www.bloggersideas.com/uk/shopify-vs-etsy-comparison/ (дата звернення: 20.12.2023)

25. Найкраща платформа електронної комерції для малого бізнесу Великобританії // [Електронний ресурс] Режим доступу до ресурсу: https://www.eworldtrade.com/blog/uk/ (дата звернення: 20.12.2023)
26. 9 найкращих програм для кошика для покупок у 2023 році🛒- Скільки коштує програмне забезпечення для кошика для покупок? // [Електронний ресурс] Режим доступу до ресурсу: https://www.bloggersideas.com/uk/best-shopping-cart-software/ (дата звернення: 20.12.2023)
27. Що таке 3PL? Основи логістики третьої сторони – визначення, значення, процес і переваги// [Електронний ресурс] Режим доступу до ресурсу: https://fulfillment-box.com/uk/shcho-take-3pl/ (дата звернення: 20.12.2023)
28. За кнопкою «Купити»: розуміння логістики електронної комерції // [Електронний ресурс] Режим доступу до ресурсу: https://www.cci.zp.ua/app/uploads/2023/08/e-logistics_aug23.pdf (дата звернення: 20.12.2023)
29. Архітектура компанії 3PL-провайдера // [Електронний ресурс] Режим доступу до ресурсу: https://flowium.com/blog/third-party-logistics/ (дата звернення: 20.12.2023)
30. 4 стратегії цифрового маркетингу для збільшення продажів в електронній комерції // [Електронний ресурс] Режим доступу до ресурсу: https://www.ranktracker.com/uk/blog/4-digital-marketing-strategies-to-boost-your-e-commerce-sales/ (дата звернення: 20.12.2023)
31. Переваги Odoo для бізнесу в сфері електронної комерції // [Електронний ресурс] Режим доступу до ресурсу: https://simpleerp.com.ua/odoo-dlia-biznesu-v-elektronnoi-komertsii (дата звернення: 20.12.2023)
32. Anticipating the Need for Virtual Unified Threat Management // [Електронний ресурс] Режим доступу до ресурсу: https://www.tatatelebusiness.com/articles/anticipating-the-need-for-virtual-unified-threat-management/ (дата звернення: 20.12.2023).
33. РОЗРОБКА ВЕБ-САЙТІВ НА E-COMMERCE: СТВОРЕННЯ ЦИФРОВОЇ ВІТРИНИ // [Електронний ресурс] Режим доступу до ресурсу:

https://redstone.media/rozrobka-veb-saitiv-na-e-commerce-stvorennia-tsyfrovoi-vitryny (дата звернення: 20.12.2023)

34. 8 важливих плагінів для вашого веб-сайту електронної комерції // [Електронний ресурс] Режим доступу до ресурсу: https://www.ranktracker.com/uk/blog/8-essential-plugins-for-your-ecommerce-business-website/ (дата звернення: 20.12.2023).
35. Соціально-економічний розвиток і безпека України: стан та перспективи: матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Львів, 23 березня 2023 р.) / за заг.ред. В.С. Бліхара, М.І. Копитко. Львів : ЛьвДУВС, 2023. 167 с. // [Електронний ресурс] Режим доступу до ресурсу: //C:/Users/%D0%B2%D0%B8%D0%B4%D0%B5%D0%BE/Downloads/23_03_2023%20(1).pdf (дата звернення: 20.12.2023).
36. 11 найкращих рішень CMP для забезпечення відповідності перед збором даних // [Електронний ресурс] Режим доступу до ресурсу: https://techukraine.net/11-%D0%BD%D0%B0%D0%B9%D0%BA%D1%80%D0%B0%D1%89%D0%B8%D1%85-%D1%80%D1%96%D1%88%D0%B5%D0%BD%D1%8C-cmp-%D0%B4%D0%BB%D1%8F-%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F-%D0%B2/#google_vignette (дата звернення: 20.12.2023).
37. ПОСЛУГИ ВІДПОВІДНОСТІ ТА УПРАВЛІННЯ // [Електронний ресурс] Режим доступу до ресурсу: https://cqr.company/ua/service/compliance-and-governance-service/ (дата звернення: 20.12.2023).
38. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– № 8 (серпень) . – 318 с. // [Електронний

ресурс] Режим доступу до ресурсу: https://ippi.org.ua/sites/default/files/2023-8.pdf (дата звернення: 20.12.2023).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ 1

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ДИПЛОМНА РОБОТА
на ступінь вищої освіти магістр
із спеціальності 122 Комп'ютерні технології

Дослідження методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce

Виконав: студент 6 курсу, групи КНДМ-62
Шуляк Андрій Олегович
Керівник: д.т.н., доцент Катков Ю.І.

Київ - 2023

2

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ДИПЛОМНОЇ РОБОТИ

Тема	Дослідження методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce
Мета дослідження	розробка комплексу рекомендацій щодо підвищення ефективності застосування методів безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce
Наукове завдання	оцінка доцільності та ефективності використання визначених методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce
Об'єкт дослідження	процес застосування методів забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.
Предмет дослідження	методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії для eCommerce.

3

АНАЛІЗ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЛАНЦЮЖКІВ ПОСТАЧАННЯ У ЛОГІСТИЧНОЇ КОМПАНІЇ THIRD-PARTY LOGISTICS ПІД ЧАС E-COMMERCE

Характеристики електронної комерції (E-COMMERCE)

1. Електронна комерція (E-COMMERCE)
2. Бізнес електронної комерції
3. Веб-сайт електронної комерції
4. Маркетинг електронної
5. Види електронної комерції.

- B2C – підприємства продають продукцію окремим споживачам (кінцевим користувачам). Найпоширеніша модель, що має безліч варіацій.
- B2B – Підприємства продають іншим підприємствам. Часто покупець перепродує продукцію споживачеві.
- C2B – споживачі продають бізнесу. Бізнес C2B дозволяє клієнтам продавати іншим компаніям.
- C2C – споживачі продають іншим споживачам. Компанії створюють онлайн-ринки, які поєднують споживачів.
- B2G – підприємства продають свою продукцію урядам чи урядовим установам.
- C2G – споживачі продають товари урядам чи урядовим установам.
- G2B – уряди чи урядові установи продають бізнесу.
- G2C – уряди чи урядові установи продають споживачам.

Методи ведення електронної комерції [1, 2, 4]:

- М-комерція.
- Корпоративна електронна комерція.
- Електронна комерція у соціальних мережах.

4

Переваги та недоліки електронної комерції

Переваги електронної комерції.

- Швидко росте.
- Пропонує глобальне маркетингове охоплення.
- Забезпечує зручність замовлення продукції через Інтернет.
- Передбачає більш низькі експлуатаційні витрати.
- Забезпечує прямий доступ до споживача.

Недоліки електронної комерції.

- Обмежене особисте спілкування..
- Технічні проблеми..
- Безпека даних..
- Проблеми доставки та виконання замовлень у великих масштабах..

Кроки реалізації доставки електронної комерції

- Приймання замовлень.
- Обробка їх.
- Упаковка купленої продукції на складі.
- Друк етикеток для цих упаковок.
- Надсилання посилок.
- Управління доходами.

5

Способи доставки електронної комерції

1. Доставка того ж дня.
2. 2-денна доставка.
3. Нічна доставка.
4. Прискорена доставка.

Інструменти доставки електронної комерції:

1. CMS
2. Shopify.
3. WooCommerce.
4. Wix.
5. BigCommerce.

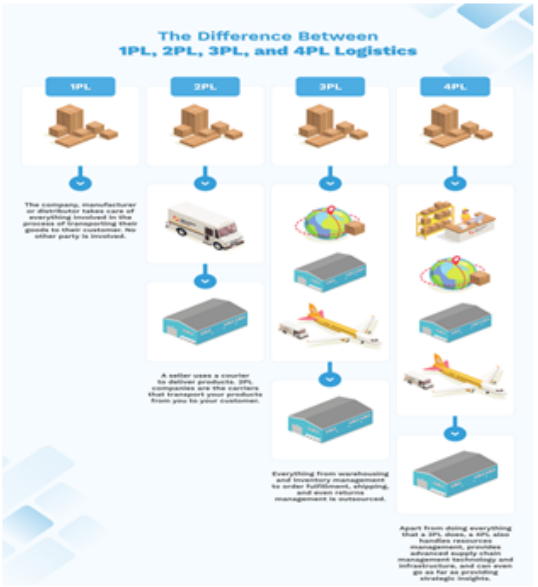
Програмне забезпечення для електронної комерції.

1. ShipStation.
2. Shippo.
3. Easyship Easyship
4. ShipEngine.
5. eHub.

6

Логістичні компанії , їх операції й функцій

Логістичні компанії – це сторонні постачальники послуг з виконання замовлень, які пропонують обробку замовлень та такі послуги, як складування, комплектування, упаковка та доставка. Логістичні компанії отримують, обробляють та зберігають товар від торговців. Прикладами логістичних компаній у США для доставки електронної комерції є FedEx, UPS, USPS, DHL, Ceva Logistics тощо.



Види логістичних компанії

1. 1PL,
2. 2PL,
3. 3PL
4. 4PL

7

Характеристики логістичних компанії

Архітектура логістичних компанії

3PL-компанії працює наступним чином:

- **Отримання**
- **Збір**
- **Упаковка**
- **Перевезення**

8

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ ДЛЯ E-COMMERCE

- Конфіденційність.
- Чесність.
- Аутентифікація.
- Невідмова від відповідальності.

Проблеми безпеки електронної комерції

1. Нестача довіри до конфіденційності та безпеки електронної комерції.
   - Підроблені сайти.
   - Шкідливі зміни веб-сайтів.
   - Крадіжка даних клієнтів..
   - Збитки комп'ютерних мереж.
   - Відмова в обслуговуванні.
   - Шахрайський доступ до конфіденційних даних.
2. Шкідливе ПЗ, віруси та онлайн-шахрайство.
3. Невизначеність та складність онлайн-транзакцій.

Методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії

9

Метод визначення стратегії захисту даних

- Запобігання втраті даних
- Шифрування
- Доступність даних.
- Управління життєвим циклом даних
- Управління життєвим циклом інформації.

Метод виконання політик (правил) захисту даних.

- політика захисту даних;
- стратегія захисту даних;
- визначаються технології та практики захисту даних для захисту приватних даних.
- виявлення даних;
- інвентаризація та класифікація даних;
- відображення даних;
- інструменти автоматизованого виявлення;
- політики запобігання втраті даних;
- моніторинг і сповіщення;
- санація;
- зберігання з вбудованим захистом даних;
- надмірність;
- виправлення помилок;
- контроль доступу;
- резервне копіювання;
- локальні та зовнішні резервні копії;
- моментальні знімки;
- миттєве відновлення;
- керування версіями;
- ефективність зберігання;
- тиражування;
- відмово стійкість;
- реплікація даних (відмова);
- балансування навантаження;
- географічна надмірність;
- брандмауери;
- контроль додатків;
- моніторинг руху;
- автентифікація та авторизація;
- багатофакторна автентифікація;
- контроль доступу на основі ролей;
- захист кінцевої точки;
- управління пристроєм;

Заходи безпеки веб-сайту електронної комерції

10

1. Використовуйте багаторівневу безпеку.
2. Отримайте сертифікати Secure Server Layer (SSL).
3. Використовуйте надійні брандмауери.
4. Дотримуйтесь вимог PCI-DSS.

Найважливіші інструменти конфіденційності даних для електронної комерції

1. Шифрування даних.
2. Анонімізація даних.
3. Управління згодою на дані.
4. Контроль доступу до даних.
5. Виявлення витоку даних та реагування на неї.
6. Навчання та підвищення обізнаності щодо конфіденційності даних.
7. Моніторинг та виявлення загроз.

11

РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ ДЛЯ E-COMMERCE

1 Рекомендації щодо застосування інтелектуальних засобів для розробки веб-сайту електронної комерції

1. Перевірка байт-коду.
2. Менеджери безпеки.
3. Завантажувачі класів.
4. Криптографія:
5. Автентифікація та авторизація.

2 Рекомендації щодо управління доступом до даних на веб-сайту електронної комерції

1. Дискреційний контроль доступу (DAC):.
2. Обов'язковий контроль доступу (MAC):
3. Контроль доступу на основі ролей (RBAC):
4. Контроль доступу на основі атрибутів (ABAC):

12

ПРОДОВЖЕННЯ РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ ДЛЯ E-COMMERCE

3 Рекомендації щодо псевдонімізації, шифрування та анонімізація даних на веб-сайту електронної комерції

1. Анонімізація. Псевдонімізацію
2. Приховування або маскування даних.
3. Шифрування

4 Рекомендації щодо застосування біометричної технології та ідентифікації користувача на веб-сайту електронної комерції

Біометрична автентифікація користувачів:

1. Розпізнавання обличчя.
2. Сканер відбитків пальців.
3. Сканери очей.
4. Розпізнавання голосу.

ПРОДОВЖЕННЯ РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ ДЛЯ E-COMMERCE

13

5 Рекомендації щодо захисту від витоків інформації та несанкціонованого доступу на веб-сайт електронної комерції

Протидія типам витоку даних:

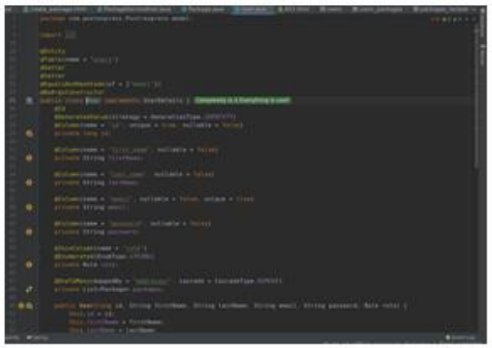
1. Людські помилки.
2. Застаріле програмне та апаратне забезпечення.
3. Фізична крадіжка.
4. Внутрішні джерела.
5. Ризик третіх осіб.
6. Шкідливі електронні повідомлення.

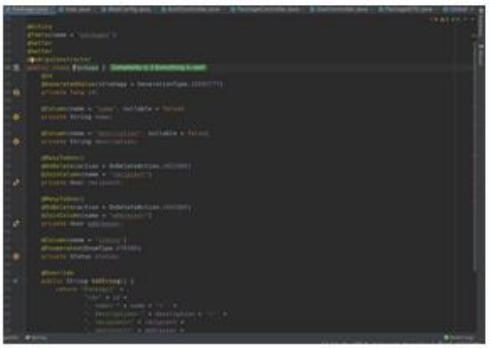
6 Рекомендації щодо захисту від соціально-інженерних атак на веб-сайт електронної комерції

1. Фішинг.
2. Списовий фішинг.
3. Заманювання.
4. Програми залякування.

Розробка Web-Додатку для логістичних компаній з використанням аутентифікації та авторизації користувача

14





АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ

15

Матеріали були опубліковані:
в статті:
Шуляк А.О. Методи забезпечення безпеки та конфіденційності даних користувача у логістичної компанії./ Ю. І. Катков, А.О.Шуляк// Наукові записки Державного університету телекомунікацій №4, 2023, Подано до друку. https://journals.dut.edu.ua/index.php/sciencenotes/issue/archive
в тезисах:
Катков Ю. І., Шуляк А. О. МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ДАНИХ КОРИСТУВАЧА У ЛОГІСТИЧНОЇ КОМПАНІЇ // Науково-практична конференція «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ» Збірник тез. – К.: ДУІКТ, 2023. 27 жовтня 2023, С- 365-369. https://duikt.edu.ua/uploads/p_2626_52007398.pdf

16

ВИСНОВКИ

Під час виконання атестаційної магістерської роботи була розглянута актуальна проблема створення логістичного додатку для мобільних працівників, диспетчерів, водіїв і кур'єрів, які займаються доставкою товарів роздрібним продавцям або клієнтам.

У процесі дослідження визначено предмет та об'єкт дослідження, проведений аналіз методів і принципів побудови систем управління логістикою. Також була розроблена система управління логістикою, строго виконуючи план розробки програмного забезпечення.

Аналізуючи недоліки та проблеми у процесі розробки веб-додатку, було поставлено завдання щодо дослідження та запропонована ефективна розробка, заснована на фреймворку Spring з підтримкою мови програмування Java.

Це дозволило досягти поставлених мет ці:

1. Підвищення ефективності розробки моделей.
2. Збільшення швидкості веб-додатку.
3. Додана аутентифікація та авторизація для користувачів.