МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ

Реєстраційний №_____
Дата _____

Трофіменков Олександр
Олександрович
студент 3 курсу
денної форми навчання
групи ІПЗ

Звіт

ПРО ПРОХОДЖЕННЯ ТЕХНОЛОГІЧНОЇ (ВИРОБНИЧОЇ) ПРАКТИКИ
Тема: «Методи та засоби оцінювання загроз та ризиків сервісу онлайн замовлень»
Спеціальність 121 Інженерія програмного забезпечення

Рекомендована до захисту
“____” _____ 2023р.
Робота захищена
“____” _____ 2023р.
з оцінкою
_____
Підписи членів комісії:
_____

Керівник практики від ВНЗ :
доц. Шпак І.І.

Ужгород – 2023

ЗМІСТ

ВСТУП

Технологічна (виробнича) практика є невід'ємною складовою частиною освітнього процесу, оскільки надає студентам можливість застосовувати свої знання та набуті навички у реальних умовах. Практика допомагає студентам отримати практичний досвід, розвинути професійні вміння, а також покращити їх адаптацію до робочого середовища.

Моя технологічна (виробнича) практика була проведена в організації ФОП «Шаранич В.В.», де основним предметом діяльності було проектування і розробка тривимірних застосувань.

Моїм індивідуальним завданням було дослідження методів та засобів оцінювання загроз та ризиків сервісу онлайн замовлень. Тема мого дослідження включала в себе класифікацію онлайн сервісів, загроз та ризиків сервісів онлайн замовлень, а також розгляд різних методологій оцінок ризиків та загроз.

Метою роботи було оволодіння та розуміння методів та засобів оцінювання загроз та ризиків сервісу онлайн замовлень, що дозволить підвищити рівень безпеки та захисту цих сервісів. Це дослідження має на меті розкриття основних елементів класифікації загроз та ризиків сервісів онлайн замовлень, а також огляд і аналіз різних методологій оцінок ризиків та загроз.

У даній роботі будуть розглянуті основні елементи класифікації онлайн сервісів та загроз та ризиків, пов'язаних з сервісами онлайн замовлень. Крім того, будуть представлені різні методології оцінок ризиків та загроз, які використовуються для виявлення та оцінки потенційних проблем та небезпек у цих сервісах. Зокрема, будуть детально розглянуті методології DREAD, STRIDE, FMEA, пенетраційне тестування, а також SWOT-аналіз та Байєсівський аналіз і Мережа Байєса як додаткові методи та засоби оцінювання загроз та ризиків.

РОЗДІЛ І. ЗАГАЛЬНА ХАРАКТЕРИСТИКА БАЗИ ПРАКТИКИ

1.1 Короткі відомості про базу практики

ФОП «Шаранич В.В.» – це спеціалізована організація з кваліфікованою командою фахівців, яка зосереджується на проектуванні і розробці тривимірних об’єктів для різних застосувань, які працюють в режимі реального часу. Діяльність організації охоплює такі напрямки:

- **Розробка систем симуляції різних процесів.** Організація займається створенням систем, що стимулюють різноманітні процеси, включаючи фізичні явища.
- **Розробка мережевих застосунків на базі архітектури P2P.**
- **Проектування VFX систем та візуальних ефектів.** Організація спеціалізується на проектуванні систем візуальних ефектів та їх інтеграції в відповідні програмні системи.
- **Розробка шейдерів для генерації текстур та візуалізації складних поверхонь.**
- **Розробка утиліт для процедурної генерації тривимірних об’єктів.**
- **Розробка тривимірних об’єктів та дизайну.** Організація спеціалізується на створенні деталізованих тривимірних об’єктів. Цей процес включає розробку форм, текстур та освітлення.

У робочому процесі організації ФОП «Шаранич В.В.» завдання розподіляються між командами фахівців наступним чином:

- **Команда з мережевого програмування.**
- **Команда з оптимізації контенту**, до якого входять тривимірні об’єкти, текстурні дані, фізичні колізії та освітленність.
- **Команда з дизайну віртуальних середовищ**, які спеціалізуються на створенні тривимірних об’єктів, віртуальних середовищ та освітлення.

РОЗДІЛ ІІ. МЕТОДИ ТА ЗАСОБИ ОЦІНЮВАННЯ ЗАГРОЗ ТА РИЗИКІВ СЕРВІСУ ОНЛАЙН ЗАМОВЛЕНЬ

2.1 Класифікація онлайн сервісів

Онлайн сервіси – це сайти, що надають різноманітні послуги через Інтернет та дозволяють значно заощадити час. Ці сервіси дозволяють користувачам здійснювати пошук або передачу інормації, проводити грошові операції, спілкуватися тощо. Онлайн сервіси можна розділити на наступні основні групи:

1. **Інформаційно пошукові** – це ресурси, які призначені для пошуку необхідної інформації за відповідною тематикою.
2. **Соціальні** – це ресурси, до яких належать різноманітні соціальні мережі, платформи для онлайн-комунікації, а також електронні поштові сервіси. Вони дозволяють користувачам спілкуватися з людьми незалежо від їх місцезнаходження, обмінюватися файлами тощо.
3. **Сервіси онлайн замовлень** – це ресурси, які призначені для покупки товарів або замовлення послуг через Інтернет.
4. **Банківські сервіси** – це ресурси, за допомогою яких можна здійснювати банківські операції в онлайн-режимі. Використовуючи ці сервіси, користувачі можуть здіснювати оплату покупок або послуг, таких як сплата комунальних послуг, без необхідності відвідувати банк особисто.

2.2 Класифікація загроз та ризиків сервісів онлайн замовлень

У сфері онлайн замовлень, існує ризик виникнення загроз, які можуть серйозно нашкодити онлайн-торгівлі. За статистикою, кожен рік сервіси онлайн замовлень стикаються з високим рівнем загроз – до 32,4% від усіх випадків. Зловмисники зазвичай націлюють свої атаки на адміністраторів, користувачів і співробітників, використовуючи різноманітні шкідливі методи. Через це в сервісі онлайн замовлень можуть виникати проблеми, такі як:

1. **Фінансові шахрайства** з використанням крадених кредитних карток та фальшивих повернень коштів.
2. **Фішинг**, коли зловмисники намагаються отримати конфіденційну інформацію від користувачів, представляючи себе як інтернет-магазин або платіжна система.
3. **Розсилання спаму**, яке може призвести до зниження безпеки та продуктивності веб-сайту.
4. **DoS та DDoS атаки**, які можуть призвести до недоступності веб-сайту для користувачів.
5. Використання **шкідливвих програм** для взлому систем і крадіжки конфіденційних даних.
6. **Силовий перебір паролів**, коли зловмисники спробують вгадати паролі для доступу до адміністративної пнелі.
7. Атаки «**Людина посередині**», коли зловмисники перехоплюють комунікацію між користувачем і веб-сайтом.
8. **Скімінг**, коли зловмисники інфікують сторінки замовлень шкідливим програмним забезпеченням для крадіжки особистих та платіжних даних клієнтів.

2.3 Методології оцінок ризиків та загроз

Методології оцінок ризику – це систематичні підходи та процеси, які використовуються для визначення та оцінки ризиків в сферах діяльності. Вони надають методи для ідентифікації, аналізу та оцінки ризиків та загроз, а також розробки стратегій щодо їх мінімізацій. Методології оцінки ризику можуть бути загальними, тобто застосовуваними в різних галузях. Або ж специфічними, призначеними для конкретного виду діяльності. Деякі методології розроблені організаціями, такими як Міжнародна організація зі стандартизції (ISO).

Основні етапи методології оцінок ризику:

- **Ідентифікація ризиків.** На даному етапі визначаються потенційні загрози, події або ситуації, які можуть призвести до небажаних наслідків або втрат.
- **Аналіз ризиків.** На даному етапі оцінюються ймовірності виникнення ризиків та визначення потенційного впливу на організацію.
- **Оцінка ризиків.** На даному етапі визначаються значення ризиків на основі результатів аналізу та інших факторів, таких як важливість, пріоритетність та можливі наслідки.
- **Розробка стратегій управління ризиками.** На даному етапі розробляються плани подій для мінімізації ризиків, включаючи прийняття запобіжних заходів та розробку планів відновлення.

2.3.1 Методології DREAD та STRIDE

DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) – це методологія оцінки ризику, яка дозволяє ідентифікувати та оцінити загрози шляхом постановки ряду запитань з використанням п’яти категорій (рис. 2.1):

1. **Шкода**. Оцінюється потенційна шкода, яка може бути завдана внаслідок реалізації загрози. Вимірюється відносними величинами, наприклад, вартістю втрати даних.
2. **Відтворюваність**. Вказує, наскільки легко можна відтворити або використати загрозу. Цей фактор оцінює ймовірність повторного виникнення або використання загрози.
3. **Експлуатованість**. Визначає, наскільки просто зловмисник може використати загрозу. Це включає оцінку складності злому, використання вразливості або отримання несанкціонованого доступу.
4. **Кількість постраждалих користувачів**. Визначає, скільки користувачів або систем можуть бути постраждалими внаслідок реалізації загрози. Цей фактор оцінює розмір впливу на організацію, її клієнтів або користувачів.
5. **Виявлення**. Оцінює ймовірність того, наскільки легко буде виявлена загроза.

Threat	**D**	**R**	**E**	**A**	**D**
Sniffing	2	2	2	3	3
Tampering	3	2	2	2	3
MITM	3	3	1	3	2
MITB	3	3	2	2	3
XSS	3	1	1	2	3

Рис. 2.1. Приклад пріорітизації загроз за моделлю DREAD

В той час методологія **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service) використовується для виявлення загроз в архітектурі додатку на ранніх стадіях, коли вартість їх усунення найменша (рис. 2.2). В результаті цього значно знижується загальна вартість розробки і покращується рівень безпеки додатка. STRIDE складається з наступних компонентів:

1. **Спуфінг.** Оцінка можливості підробки ідентифікації або авторизації в системі.
2. **Підробка.** Оцінка можливості зміни, підроби або незаконного доступу до даних в системі. Це може включати атаки «людина посередині», де зловмисник перехоплює та змінює передані дані.
3. **Заперечення.** Оцінка можливості заперечення або відмови користувача від відповідальності за виконані дії або транзакції.
4. **Розкриття інформації.** Оцінка можливості незаконного розкриття конфіденційної інформації. Це може включати аналіз алгоритмів захисту персональних даних користувачів та передачі даних по мережі.
5. **Недоступність сервісу.** Оцінка можливості атаки, яка призводить до відмови в обслуговуванні для користувачів.

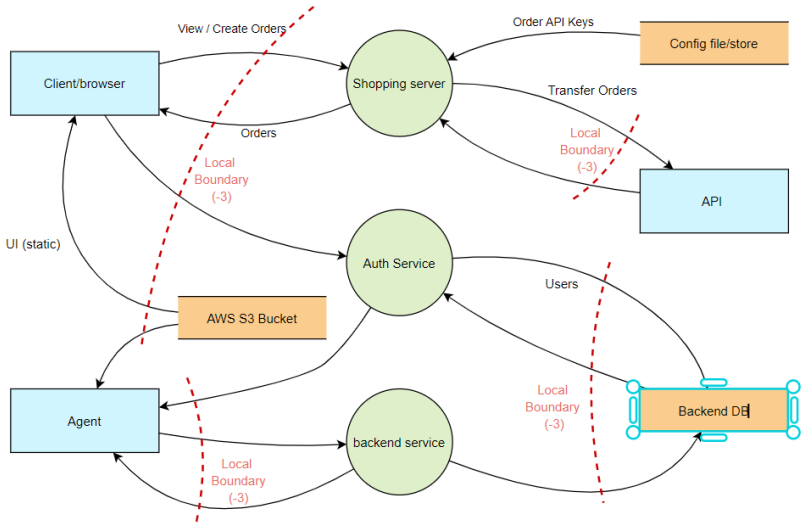

Рис. 2.2. Приклад моделювання загроз STRIDE

2.3.2 Виконання пенетраційного тестування

Пенетраційне тестування – це метод оцінення захищенності комп’ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників і внутрішніх зловмисників [4]. Його основна мета – виявити вразливості та слабкі місця в системі, які можуть бути використані зловмисниками для несанкціонового доступу, зміни даних або виконнання інших шкідливих дій.

Існують такі види пенетраційного тестування:

1. **Соціальна інженерія** – це вид тестування з підключенням «людського контингенту» [4], за допомогою якого можна оцінити вразливість працівників компанії до маніпуляцій та обману. Зловмисники можуть використовувати соціальну інженерію для отримання несанкціонованого доступу до системи або конфіденційних даних. Прикладами таких атак є фішинг або виманювання інформації по телефону.
2. **Тестування веб-додатків –** це вид тестування, який спрямований на оцінку безпеки веб-додатків і сервісів. Його мета полягає у виявлені загроз, таких як недостатня автентифікація, валідація даних тощо.
3. **Тестування на віддалене підключення** – це вид тестування, за допомогою якого оцінюється безпека з’єднань VPN. Вразливості можуть стосуватися слабких алгоритмів шифрування, витоку IP-адреси тощо.

Пенетраційне тестування включає кілька етапів, які допомагають оцінити безпеку системи та виявити потенційні вразливості. Основні послідовні етапи пенетраційного тестування включають:

- **Аналіз відкритих джерел**. На цьому етапі збирається публічна інформація про організацію. Це можуть бути дані з веб-сайту, соціальних мереж тощо. Мета такого аналізу є виявлення ризиків та можливих шляхів атак з використанням публічних даних.

- **Інструментальне сканування**. На цьому етапі використовуються спеціальні інструменти для сканування системи з метою виявлення вразлисвостей.
- **Аналіз та оцінка виявлених вразливостей і вироблення рекомендацій**. На цьому етапі виявлені вразливості оцінюються щодо їх впливу на систему та ризику для організації.

На етапі оцінки виявлених вразливостей в пенетраційному тестуванні зазвичай використовується методологія **Common Vulnerability Scoring System** (**CVSS**).

Common Vulnerability Scoring System – це система, яка призначена для оцінювання загроз та ризиків програмного забезпечення. Вона використовується для надання оцінки рівня загрози для системи або організації. CVSS дозволяє стандартизувати опис вразливостей та прогнозувати їх вплив на систему з використанням числових показників. Існують такі три основні метрики:

1. **Базові метрики**, які включають показники з відображенням основних аспектів вразливості. Вони скаладаються з двох наборів, такі як:
   - **Показники експлуатації**, що включають в себе вектор атаки, складність атаки, потрібні привілеї та взаємодію з користувачем.
   - **Показники впливу**, що включають в себе вплив на конфіденційність, вплив цілісності та вплив доступності.
2. **Тимчасові метрики**, які враховують змінювані з часом фактори.
3. **Окремі метрики**, які дозволяють оцінити серйозність впливу вразливості на систему при її використанні.

Оцінка CVSS (походить за шкалою від 0 до 10, де 10 є найвищим рівнем загрози. Базова метрика є обов'язковою в цьому процесі, тоді як тимчасова – необов'язковою. Обидві оцінки надаються розробником програмного забезпечення або аналітиком. Далі користувач самостійно розраховує середовищну оцінку, яка також є необов'язковою.

Окрема метрика є більш складним розрахунком. Користувач повторно обчислює базову та тимчасову метрики, використовуючи п'ять обчислень для більш точної оцінки серйозності загрози.

Рис. 2.3. Діапазон оцінок CVSS

Також іноді використовуєтья автоматизований інструмент під назовою **Web Application Mapper (WMAP)** для виявлення потенційних загроз та оцінки рівня безпеки веб-додатків. Він дозволяє проводити сканування веб-додатків (рис. 2.4), їх сторінок і аналізувати їх структуру, щоб виявити різноманітні вразливості, які можуть бути використані зловмисниками.

Одна з ключових можливостей WMAP полягає у виявлені вразливостей введення даних. Він перевіряє, як додаток обробляє та перевіряє дані, введені користувачами, щоб виявити потенційні проблеми, такі як SQL-ін'єкція або некоректна обробка файлів.

Крім того, WMAP аналізує доступ до ресурсів веб-додатків і перевіряє наявність вразливостей в контексті авторизації та контролю доступу. Він виявляє можливі слабкі місця, які можуть дозволити несанкціонованим користувачам отримати доступ до обмежених ресурсів або функціоналу.

Також, WMAP перевіряє наявність конфіденційної інформації, такої як паролі, кредитні картки чи інші чутливі дані, що можуть бути недостатньо захищені.

Додатково, WMAP може надати повний звіт про всі виявлені загрози, який містить детальну інформацію про вид загрози, її серйозність та рекомендації щодо виправлення вразливості для підвищення рівня безпеки.

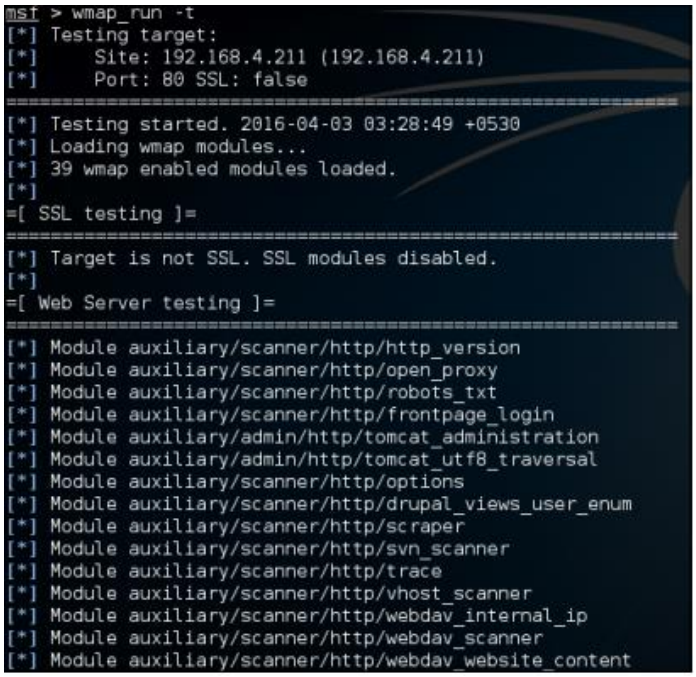

Рис. 2.4. Приклад використання WMAP

2.3.3 Методологія FMEA

Методологія FMEA – це інструмент, за допомогою якого можливо оцінити потенційні загрози, помилки та ризики у процесі або продукті з метою їх запобігання або управління (рис. 2.5).

Процес FMEA складається з наступних кроків:

1. **Визначення об'єкту аналізу** – етап на якому визначаються об'єкти, які підлягають оціці. Це можуть бути процеси, продукти або послуги.
2. **Визначення потенційних помилок** – етап на якому кожен об'єкт аналізується для визначення можливих загроз та ризиків.
3. **Визначення причин виникнення** – етап на якому для кожної загрози визначаються можливі причини виникнення.
4. **Визначення можливих наслідків** – етап на якому визначаються можливі наслідки у випадку виникнення загрози.
5. **Оцінювання ризиків** – етап на якому виконується оцінка ризиків з використанням підхіду SxOxD, де:
    - **S (тяжкість)** – оцінювання наслідків в результаті відмови системи.
    - **O (виникнення)** – оцінювання ймовірності виникнення відмови.
    - **D (виявлення)** – оцінювання здатності оперативно виявити помилки або відмови.
6. **Визначення засобів вирішення проблеми** – етап на якому для об'єкту аналізу розробляються засоби вирішення проблеми або заходи контролю.

FMEA (Failure Mode and Effects Analysis)
Аналіз потенційних помилок і їх наслідки

Об'єкт аналізу	Потенційні помилки	Причини виникнення помилки	Можливі наслідки	S	O	D	SxOxD оцінювання ризику	Засоби вирішення проблеми	Відповідальний, дата
Сервіс онлайн замовлень	Втрата зв'язку з сервером	Технічна несправність сервера	Неможливість обробки замовлень	7	4	8	224	Резервне копіювання даних	IT-відділ, 01.01.2023

Рис. 2.5. Приклад використання методології FMEA

2.4 Додаткові методи та засоби оцінювання загроз та ризиків

В даному розділі будуть розглянуті додаткові методи та засоби, до яких входять статистичні та системні методи, які можуть бути застосовані з іншими засобами для оцінювання заагроз та ризиків.

Системні методи – це методи, які використовуються для дослідження та аналізу складних систем з метою розуміння їх структури, взаємодій компонентів і функціонування. Вони використовуються для вивчення та оцінки системних проблем і виявлення оптимальних стратегій для вирішення проблем.

Статистичні методи – це набір математичних та аналітичних інструментів, які використовуються для збору та аналізу даних з метою правильно оцінити проблему та прийняти рішення на основі ймовірностей та статистичних закономірностей.

Експертні методи – це методи, які базуються на знаннях і досвіді експертів у певній галузі. Використання експертного методу передбачає залучення кваліфікованих фахівців, які мають глибокі знання та розуміння відповідної проблематики для подальшої оцінки та знаходження рішення.

Експертні методи можна розділити на такі групи:

- **Метод програмного прогнозування**. Використовується для визначення ймовірності настання подій та оцінки ймовірного часу їх настання.
- **Метод евристичного прогнозування**. Використовується для обробки оцінок шляхом систематичного опитування експертів.
- **Метод колективної генерації ідей**. Використовується для створення нових та інноваційних ідей експертами під час вільного висловлювання ідей без обмежень та критики, з метою знаходження творчих рішень та оцінок проблем.

2.4.1 SWOT-аналіз

SWOT-аналіз (рис. 2.6) – це найпоширеніший аналітичний інструмент, який допомагає організаціям виявити їх сильні сторони та слабкі місця, оцінити загрози та проблеми, які впливають на їхню діяльність.

Рис. 2.6. Макет SWOT-аналізу

Матриця SWOT містить такі складові:

1. **S (Strengths)** – це складова, яка включає список сильних сторін компанії або організації. Сильні сторони вказують на переваги сервісу, особливості тощо. Наприклад, це може бути високий асортимент товарів або якісна продукція.
2. **W (Weaknesses)** – це складова, яка включає список виявлених слабких сторін компанії або організації. Слабкі сторони вказують на недоліки, які можуть негативно впливати на функціонування організації. Наприклад, це можуть бути малокваліфіковані робітники, що може спричинити втрату клієнтів та погіршення репутації сервісу.
3. **O (Opportunities)** – це складова, в якій описуються можливості сервісу. Вони вказують на потенційні переваги для розвитку бізнесу. Наприклад, зростання популярності сервісу онлайн замовлень.

4. **T (Threats)** – це складова, яка включає список виявлених загроз та ризиків, що можуть негативно вплинути на діяльність компанії або організації. Існує два основних типи загроз:
    - **Загроза для компанії**: Наприклад, конкуренція з боку великих компаній, які мають репутацію та широкий асортимент товарів.
    - **Загроза для користувачів**: Наприклад, шахрайство. Зловмисники можуть створювати підроблені веб-сайти щоб отримати конфіденційні дані користувача та гроші без надання товарів або послуг.

STRENGTHS	**WEAKNESSES**
Широкий асортимент товарів;	Висока залежність від інтернет-з'єднання;
Швидкість замовлення;	Можливі технічні проблеми;
OPPORTUNITIES	**THREATS**
Зростання популярності онлайн замовлень;	Значна конкуренція;
Розширення асортименту товарів;	Збільшення шахрайства;

Рис. 2.7. Приклад простого варіанту SWOT-аналізу

2.4.2 Байєсівський аналіз і Мережа Байєса

Байєсівський аналіз – це статистичний метод, який базується на теоремі Байєса та дозволяє оцінювати ймовірності подій на основі наявних даних та апріорних знань. Також, він може використаний для оцінювання ризиків та прийняття рішень з використанням ймовірнісних моделей.

Мережа Байєса – це графічна модель, яка відображає залежності між різними подіями або змінними та використовує Байєсівський аналіз для оцінювання ймовірностей. Наприклад, для визначення ймовірності ризикових подій та їх взаємозв'язків для прийняття рішень щодо управління ризиками.

Основна формула (рис. 2.8) для оцінки повної ймовірності, відома як теорема Байєса, виражає залежність між апостеріорною ймовірністю, апріорною ймовірністю, ймовірністю спостереження при наявності додаткової події та ймовірністю без урахування додаткової події [8].

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)}$$

Рис. 2.8. Напройстіша форма теореми Байєса

Приклад використання

Мережу Байєса можна використовувати для моделювання різних факторів ризику, таких як шахрайство, виток даних тощо. Застосовуючи теорему Байєса, можна оновлювати ймовірності цих ризиків на основі отриманих спостережень та попередніх знань.

Наприклад, якщо апріорна ймовірність випадку шахрайства 0.01, ймовірність позитивного результату перевірки шахрайства 0.9, ймовірність позитивного результату перевірки у випадку відсутності шахрайства 0.05, а ймовірність спостереження позитивного результату 0.07, то можна оцінити апостеріорну ймовірність випадку шахрайства (рис 2.Номер):

$$P(\text{шахрайство}|\text{позитивний результат}) = (0.9*0.01)/0.07 = 0.1286$$

Таким чином, апостеріорна ймовірність випадку шахрайства при отриманні позитивного результату становить 0.1286 або 12.86% і 0.8714 або 87.14% для випадку відсутності шахрайства.

	Апріорна ймовірність	Ймовірність позитивного результату	Ймовірність позитивного результату без шахрайства	Ймовірність спостереження позитивного результату	Апостеріорна ймовірність
Шахрайство	0.01	0.9	0	-	**0.1286**
Відсутність шахрайства	0.99	0.05	1	-	**0.8714**

Рис. 2.9. Таблиця результатів обчислень Байєсівського аналізу

ВИСНОВКИ

У результаті виконання індивідуального завдання з теми "Методи та засоби оцінювання загроз та ризиків сервісу онлайн замовлень" були розкриті основні аспекти оцінювання загроз та ризиків, пов'язаних з сервісами онлайн замовлень. В процесі виконання було вивчено класифікацію онлайн сервісів, загроз та ризиків, а також методології оцінок ризиків та загроз. В першому розділі була надана загальна характеристика бази практики з короткими відомостями.

У другому розділі було проведено класифікацію онлайн сервісів, що дозволило категоризувати їх за специфікою функціональності та ризиками. Також була розглянута класифікація загроз та ризиків, пов'язаних з цими сервісами. Також були описані відомості про методології оцінок ризиків та загроз, а також детальний опис методологій DREAD та STRIDE, які використовуються для оцінки ризиків у програмному забезпеченні. Також була наведена інформація про пенетраційне тестування як один із методів оцінки загроз та ризиків. Для систематизації і аналізу ризиків була представлена методологія FMEA.

Крім того, було розглянуто додаткові методи та засоби оцінювання загроз та ризиків, зокрема SWOT-аналіз та Байєсівський аналіз з використанням Мережі Байєса. Ці методи допомагають виявити і аналізувати ризики, пов'язані з сервісами онлайн замовлень.

В результаті досліджень було показано, що для ефективного оцінювання загроз та ризиків сервісу онлайн замовлень необхідно застосовувати комплексний підхід, використовуючи різноманітні методології та інструменти.

Посилання на репозиторій GitHub зі звітом в електронній формі: https://github.com/trofimenkov/practice2023

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. [Електронний ресурс] – Класифікація онлайн сервісів – https://avada-media.ua/ua/services/on-line-servisy/
2. [Електронний ресурс] – Класифікація загроз та ризиків сервісів онлайн замовлень – https://www.getastra.com/blog/knowledge-base/ecommerce-security-threats/
3. [Електронний ресурс] – Документація SWOT-аналіз – https://esputnik.com/uk/blog/swot-analiz-iz-prikladami
4. [Електронний ресурс] – Документація пенетраційного тестування – https://uk.wikipedia.org/wiki/Тест_на_проникнення
5. [Електронний ресурс] – Документація STRIDE – https://en.wikipedia.org/wiki/STRIDE_(security)
6. [Електронний ресурс] – Документація DREAD – https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)
7. [Електронний ресурс] – Порівняння STRIDE з DREAD – https://haiderm.com/stride-threat-modelling-vs-dread-threat-modelling/
8. [Електронний ресурс] – Байєсівський аналіз і мережа Байєса – https://moodle.znu.edu.ua/pluginfile.php/875851/mod_resource/content/1/Тема%206%20ВИБІР%20МЕТОДІВ%20ОЦІНКИ%20РИЗИКУ.pdf
9. [Електронний ресурс] – Байєсівський аналіз і мережа Байєса – https://www.management.com.ua/qm/qm262.html
10. [Електронний ресурс] – Документація експертних методів оцінювання – https://uk.wikipedia.org/wiki/Експертні_методи_оцінювання
11. Prakhar Prasad. Mastering Modern Web Penetration Testing. Packt Publishing, 2016. 298 p.