НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ Дмитро ЛАНДЕ

(підпис)

«_____»_____2024 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Модель оцінки загроз CRM-системи на основі методології STRIDE
Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-04 (шифр групи)

Андрійчук Анастасія Юріївна

(прізвище, ім'я, по батькові) (підпис)

Керівник доцент каф. ІБ Барановський О. М.

(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____

(підпис)

Київ – 2024 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2024 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Андрійчук Анастасії Юріївни

(прізвище, ім'я, по батькові)

1. Тема роботи " Модель оцінки загроз CRM-системи на основі методології STRIDE " ,
керівник роботи Барановський Олексій Миколайович, доцент кафедри ІБ.
затверджені наказом по університету від «31» травня 2024 р. No 2251-с.2.

2. Термін подання здобувачем вищої освіти роботи 12 червня 2024 р.

3. Вихідні дані до роботи: CRM-система та її компоненти

4. Зміст роботи: У цій роботі розглядається, яким можливим загрозам піддатні CRM-системи, як за допомогою яких методології STRIDE можна визначити потенційні загрози та як обрахувати ризики цих загроз. Також реаліазація застосунку для визначення рівня зрілості компанії стосовно кіберзагроз на основі проведених досліджень

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): презентація

6. Дата видачі завдання: 15 вересня 2023 року

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Терміни виконання етапів дипломної роботи	Примітка
1	Отримання завдання	15.09.23	виконано
2	Формулювання теми дипломної роботи	30.09.23	виконано
3	Постановка задач для виконання роботи	07.10.23	виконано
4	Пошук інформаційних джерел	15.10.23-15.11.23	виконано
5	Проведення досліджень та реалізація рішень	1.01.24-15.03.04	виконано
6	Оформлення дипломної роботи згідно методичних вказівок	1.05.24	виконано
7	Оформлення ілюстративниї матеріалів	10.05.24	виконано
8	Передзахист дипломної роботи	12.06.24	виконано
9	Захист дипломної роботи	19.06.24	

Здобувач вищої освіти _____ Анастасія АНДРІЙЧУК

Керівник роботи _____ Олексій БАРАНОВСЬКИЙ

РЕФЕРАТ

Дана робота обсягом 60 сторінок, включає 17 рисунків, 17 таблиць, 1 додаток та містить посилання на 21 джерело літератури.

Об’єктом дослідження є CRM-система, яка використовується для управління взаємовідносинами з клієнтами, включаючи зберігання та обробку персональних даних

Предметом дослідження є процеси і механізми виявлення та оцінки загроз для CRM-системи за допомогою методології STRIDE

Метою роботи є зменшення ризиків для даних компанії, які зберігаються в CRM-системах шляхом моделювання загроз за методологією STRIDE, а також забезпечити ефективне оцінювання зрілості компанії щодо кіберзагроз.

В ході виконання роботи було визначено загрози, яким можуть піддаватись CRM-системи та які ризики вони несуть за допомогою методології STRIDE. Також було проведено оцінювання загроз для визначення найбільш пріорітетної загрози і на основі цього було складено перелік заходів, які необхідно вжити для пом’якшення впливу загрози і її уникнення. Також, була розроблена програма для визначення рівня зрілості компанії відносно кіберзагроз опираючись на їх можливі впливи та виникнення відповідно методології STRIDE. Представлено рекомендації щодо покращення захисту систем

Ключові слова: CRM-система, методологія STRIDE, моделювання загроз

ABSTRACT

This work, consisting of 60 pages, includes 17 illustrations, 17 tables, 1 appendix, and references to 21 sources.

The object of the research is the CRM system used for managing customer relationships, including the storage and processing of personal data.

The subject of the research is the processes and mechanisms for identifying and assessing threats to the CRM system using the STRIDE methodology.

The goal of the work is to reduce risks to company data stored in CRM systems by modeling threats using the STRIDE methodology and to ensure effective assessment of the company's maturity regarding cyber threats.

In the course of the work, threats that CRM systems may face and the risks they pose were identified using the STRIDE methodology. Threat assessment was also conducted to determine the most prioritized threat, and based on this, a list of measures was compiled to mitigate and avoid the threat's impact. Additionally, a program was developed to determine the company's maturity level concerning cyber threats based on their potential impacts and occurrence according to the STRIDE methodology. Recommendations for improving the system's protection are presented.

Keywords: CRM-system, STRIDE method, threat modeling

ЗМІСТ

Перелік умовних позначень, символів, скорочень і термінів.....7

Вступ.....8

1 Загрози CRM-системи.....9

1.1 Загальні поняття та призначення CRM.....9

1.2 Основні загрози.....11

1.3 Вплив загроз на бізнес-процеси.....13

1.4 Загальний огляд методів моделювання та оцінки загроз.....14

1.5 Порівняння методів.....19

Висновки до розділу 1.....24

2 Модель загроз CRM-системи на основі STRIDE.....25

2.1 Переваги використання методології STRIDE.....25

2.2 Визначення загроз.....28

2.3 Оцінка ризиків.....41

Висновки до розділу 2.....44

3 Методи підвищення захищення CRM системи.....45

3.1 Модель визначення зрілості компанії відносно кіберзагроз.....46

3.2 Програмна реалізація моделі для визначення зрілості компанії відносно кіберзагроз.....48

3.3 Пропозиції підвищення захищенності систем.....51

3.4 Структура впровадження заходів безпеки.....52

Висновки до розділу 3.....53

Висновки.....54

Перелік джерел посилань.....56

Додаток.....58

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

CRM - Customer Relationship Management, система управління відносинами з клієнтами

IDS - Intrusion Detection System, система виявлення вторгнень

IPS - Intrusion Prevention System, система запобігання вторгнень

GDPR - General Data Protection Regulation, загальний регламент про захист даних

ISO - International Organization for Standardization, Міжнародна організація зі стандартизації

Nist - National Institute of Standards and Technology, Національний інститут стандартів і технології

Mfa - Multi-factor authentication, Багатофакторна автентифікація

ПЗ – програмне забезпечення

ШІ – штучний інтелект

ВСТУП

У сучасному бізнес-середовищі CRM-системи відіграють ключову роль у забезпеченні ефективної взаємодії між компанією та її клієнтами. Вони дозволяють зберігати та аналізувати велику кількість даних про клієнтів, що сприяє покращенню обслуговування, збільшенню продажів та оптимізації бізнес-процесів. Однак, як і будь-яка інша інформаційна система, CRM-системи піддаються численним кіберзагрозам, які можуть поставити під загрозу конфіденційність, цілісність та доступність даних.

Однією з ефективних методологій для ідентифікації та оцінки загроз є STRIDE, яка була розроблена компанією Microsoft. Методологія STRIDE дозволяє систематично підходити до аналізу загроз

У даній роботі я розглянула застосування методології STRIDE для оцінки загроз CRM-систем. Метою є створення моделі оцінки загроз, яка допоможе виявити вразливі місця системи та визначити рівень зрілості компанії у контексті кіберзагроз. Відповідно до цієї методології, було проведено детальний аналіз можливих загроз, оцінка їх критичності та розробка рекомендацій щодо зменшення ризиків.

Об’єктом дослідження є CRM-система, яка використовується для управління взаємовідносинами з клієнтами, включаючи зберігання та обробку персональних даних

Предметом дослідження є процеси і механізми виявлення та оцінки загроз для CRM-системи за допомогою методології STRIDE

Метою роботи є зменшення ризиків для даних компанії, які зберігаються в CRM-системах шляхом моделювання загроз за методологією STRIDE, а також забезпечити ефективне оцінювання зрілості компанії щодо кіберзагроз

Таким чином, дане дослідження спрямоване на підвищення рівня безпеки CRM-систем, що є надзвичайно важливим для забезпечення стабільної та ефективної роботи компаній в умовах сучасних кіберзагроз.

1 ЗАГРОЗИ CRM-СИСТЕМИ

CRM система є ключовим інструментом для сучасних бізнесів, допомагаючи управляти клієнтськими відносинами та підтримувати ефективні бізнес-процеси. Проте, разом зі своїми перевагами, вона також піддається різноманітним загрозам, які можуть виникати від зовнішніх атак, внутрішніх помилок або недбалості в обслуговуванні та захисті даних.

Методи моделювання та оцінки загроз дозволяють не лише ідентифікувати потенційні ризики для CRM системи, але і зрозуміти їх вплив на бізнес-процеси. Це важливо для того, щоб розробляти ефективні стратегії захисту, запобігання і відновлення у разі інцидентів. Порівняння різних методів дозволяє вибрати найбільш підходящий під конкретні потреби компанії, забезпечуючи оптимальний рівень безпеки та функціональності CRM системи.

1.1 Загальні поняття та призначення CRM

CRM-системи (Customer Relationship Management) - це програмні рішення, призначені для управління взаємовідносинами з клієнтами. Вони допомагають організаціям автоматизувати та оптимізувати процеси взаємодії з клієнтами на всіх етапах їхнього життєвого циклу, починаючи від першого контакту і закінчуючи післяпродажним обслуговуванням. CRM-системи забезпечують зберігання та організацію інформації про клієнтів, включаючи їх контактні дані, історію взаємодій та уподобання. Вони також забезпечують управління запитами клієнтів, відстеження вирішення проблем і надання підтримки через різні канали, такі як телефон, електронна пошта або чат. Крім того, CRM-системи дозволяють збирати та аналізувати дані про взаємодію з клієнтами для підвищення ефективності бізнес-процесів та прийняття обґрунтованих рішень.

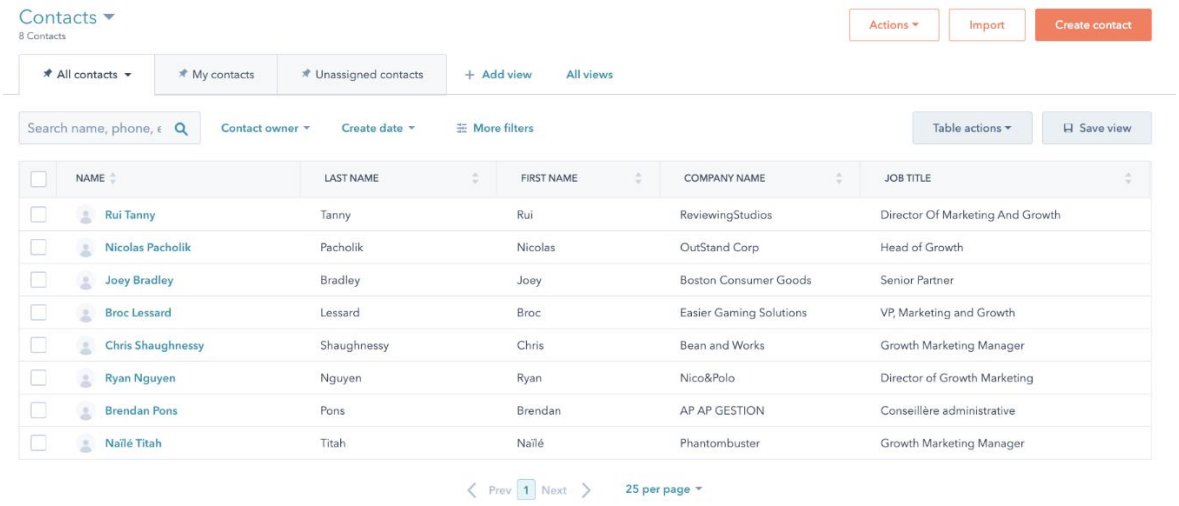

Рисунок 1.1 – Вигляд CRM з даними

CRM-системи є ключовим інструментом для сучасних бізнесів, оскільки вони допомагають ефективно керувати взаємодією з клієнтами та підтримувати високий рівень сервісу, а найголовніше вони зберігають всі дані в одному місці, які є критично важливими для функціонування підприємств.

Можна виділити наступні призначення CRM:

- Автоматизація процесів – вони автоматизують всі бізнес-процеси, такі як управління продажами, комунікація з клієнтами, сервісне обслуговування, обрахунки витрат та надходжень.
- Збереження інформації - зберігає всі дані про клієнтів в одному місці, що дозволяє легко отримувати доступ до необхідної інформації та уникати втрат даних.
- Аналіз та звітність – за допомогою CRM можна створювати та аналізувати звіти, яку стосуються роботи та фінансів, а також це допомагає контролювати потоки даних та аналізувати чи всі процеси захищені та не несуть втрат.

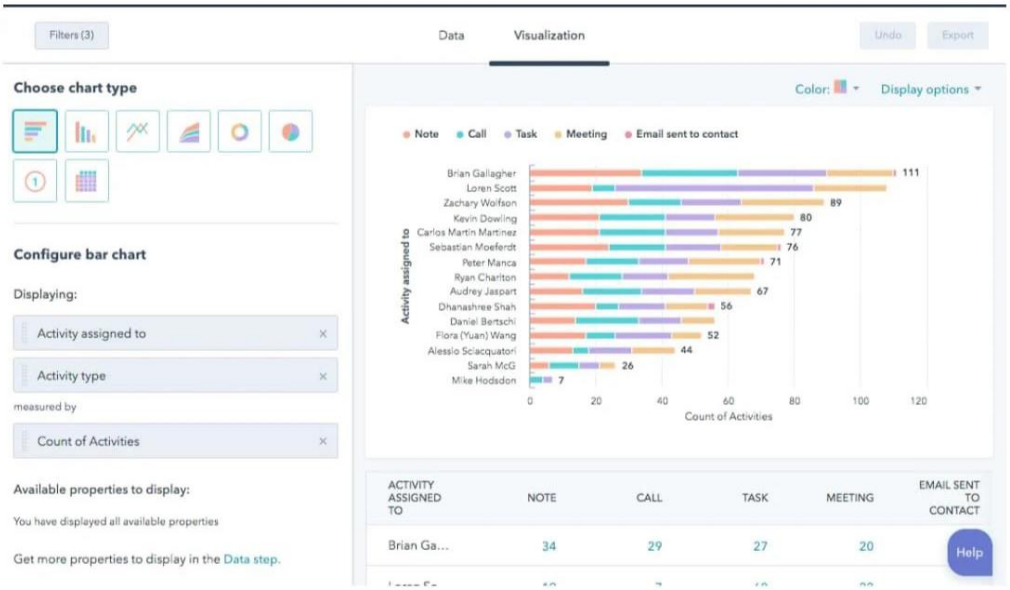

Рисунок 1.2 – Візуалізація зібраних даних діаграмою

Основна перевага CRM – це те, що вона може принести користь будь-якому підприємству та будь-якій організаційній структурі – від виробництв до впровадження таких систем у державних структурах. Оскільки CRM забезпечує швидкий доступ до даних, користувачам стає набагато простіше співпрацювати між собою - як наслідок, вирішуються питання командної взаємодії та підвищується продуктивність.

1.2 Основні загрози

CRM системи мають два типи: хмарні та локальні. Якщо організація використовує хмарну систему, то вона є більш надійною та захищеною, оскільки вона зберігає дані на серверах сертифікованого хмарного провайдера. У цьому випадку користувачі мають повний доступ до бази даних, де б вони не знаходилися. Постачальник несе відповідальність за безперебійну роботу системи і забезпечує всі необхідні оновлення та підтримку. Також, хмарні системи

зазвичай використовують регламент GDPR та стандарт ISO 27001 для забезпечення захисту даних.

Але також можливе використання локальних систем. Організації, які використовують локальну CRM, зазвичай створюють її власноруч. Компанія AIM, CRM якої я використовувала для дослідження також в процесі розробки власної, тому працюючи з нею, я виділила наступні загрози:

Зовнішні загрози – злом та крадіжка даних, фішингові атаки, інфікування системи шкідливим ПЗ. Хакери можуть спробувати проникнути в систему для викрадення конфіденційної інформації про клієнтів, включаючи персональні дані, фінансову інформацію та історію транзакцій, а також можуть використовувати фальшиві електронні листи або вебсайти, щоб отримати доступ до облікових даних користувачів CRM-системи.

Внутрішні загрози – неправомірний доступ, втрата даних. Неправильне використання CRM-системи або випадкове видалення даних може призвести до втрати важливої інформації. Також, потрібно зважати на те, що є окрема категорія загрози всередині компанії – це невдоволені працівники. Колишні або нинішні співробітники, які мають доступ до CRM-системи, можуть зловживати своїми правами для викрадення або видалення даних.

Технічні загрози - вразливості у вихідному коді, проблеми з інтеграцією. Недоліки в програмному забезпеченні CRM можуть бути використані хакерами для отримання несанкціонованого доступу. Інтеграція CRM-системи з іншими системами, які мають слабкі заходи безпеки, може призвести до витоку даних або вразливості.

На мою думку, найбільш критичними для даної CRM є кібератаки та шкідливе ПЗ. Кібератаки — це навмисні спроби хакерів або кіберзлочинців націлитися на системи CRM і використати їх вразливі місця. Вони можуть використовувати різні методи, такі як ін’єкції SQL або атаки на відмову в

обслуговуванні, щоб отримати несанкціонований доступ, викрасти конфіденційні дані або порушити роботу.

Зловмисне програмне забезпечення – це шкідливе програмне забезпечення, яке заражає системи CRM і спричиняє пошкодження або збої. Вони можуть включати віруси, хробаки, трояни, програми-вимагачі, шпигунські та рекламні програми. Воно може скомпрометувати дані, пошкодивши, видаливши, зашифрувавши або передавши їх неавторизованим особам.

Порушення даних CRM включає несанкціонований доступ або розкриття даних CRM зловмисним елементам. Це відбувається через слабке місце в захисті системи CRM, наприклад слабкі паролі.

За статистикою: 85% порушень пов’язані з людським фактором, а 61% порушень пов’язані із слабкими обліковими даними. Це може призвести до короткострокових і довгострокових фінансових втрат, таких як розслідування та пом’якшення порушення, потенційні судові позови, регулятивні штрафи тощо.

1.3 Вплив загроз на бізнес-процеси

Бізнес ризики – це ризики впливу на компанію або організацію, які призведуть до зниження її прибутків або до краху. Все, що загрожує здатності компанії досягати своїх фінансових цілей, вважається бізнес-ризиком. Зазвичай причина ризику є зовнішні загрози для компанії. Через це організація не може повністю захиститися від загроз.

Чотири основні типи ризику, з якими стикаються підприємства, це стратегічний, комплаєнс (регуляторний), операційний і репутаційний. Ці ризики можуть бути спричинені зовнішніми та внутрішніми факторами компанії

Загрози безпеки, що стосуються CRM-систем, можуть мати значний вплив на різні аспекти бізнесу. Враховуючи вплив, який загрози CRM-систем можуть

мати на бізнес, компанії повинні активно працювати над захистом своїх даних та систем. Стосовно компанії AIM можна виділити наступні загрози для бізнес-процесу:

- Відмова в обслуговуванні. Зовнішні атаки, такі як DDoS, або технічні несправності можуть призвести до недоступності CRM-системи це впливатиме на збої роботи системи та неможливість обробки важливих бізнес робіт – дзвінків, розсилки листів.
- Втрата даних. Неправомірний доступ до системи та кібератаки призводять до втрати даних, що в майбутньому нестиме репутаційні та фінансові збитки.
- Зниження продуктивності. Збої в системі будуть впливати на сповільнення робочих процесів, що впливатиме на продуктивність працівників та компанії вцілому.
- Підвищення витрат. Для термінового відновлення роботи системи або впровадження додаткових заходів реагування, необхіадно впроваджувати нові системи, які можуть вимагати значних інвестицій

Для того, щоб ефективно запобігати потенційним загрозам необхідно враховувати методології загроз та їх оцінку для майбутнього складання плану реагувань.

1.4 Загальний огляд методів моделювання та оцінки загроз

Методи моделювання загроз

Моделювання загроз — це проактивна стратегія для оцінки загроз кібербезпеці. Це передбачає визначення потенційних загроз і розробку тестів або процедур для виявлення цих загроз і реагування на них. Це передбачає розуміння

того, як загрози можуть впливати на системи, класифікувати загрози та застосовувати відповідні контрзаходи.

Типовий процес моделювання загроз включає п’ять етапів: огляд можливих загроз, ідентифікація загроз, варіанти зменшення загроз, оцінка ризиків і картування загроз. Кожне з них надає різне уявлення та бачення стану безпеки організації.

Моделювання загроз відіграє вирішальну роль у зменшенні ризиків. Виявляючи потенційні загрози до того, як їх можна буде використовувати, організації можуть вживати контрзаходів для усунення або зменшення цих ризиків. Це набагато економічно ефективніше, ніж реагувати на порушення або атаку після того, як це сталося. Крім того, розуміючи потенційні вектори атак, організації можуть із самого початку розробляти більш безпечні системи та програми.

Є вісім основних методологій, які групи безпеки можуть використовувати під час моделювання загроз: STRIDE, PASTA, VAST, Trike, CVSS, Attack Trees, Security Cards і hTMM. Кожна з цих методологій надає різні способи оцінки загроз, з якими стикаються організації. Розгляну найбільш популярні, а саме STRIDE, PASTA, VAST, Trike та Attack Trees.

STRIDE - це модель загроз, створена інженерами Microsoft, призначена для керування виявленням загроз у системі. Використовується разом з моделлю цільової системи. Це робить його найбільш ефективним для оцінки окремих систем.

PASTA - це методологія, орієнтована на зловмисників, із семи кроків. Він призначений для співвіднесення бізнес-цілей з технічними вимогами. Кроки PASTA допомагають командам динамічно визначати, підраховувати та визначати пріоритети загроз. Кроки моделі загрози PASTA:

- Визначити бізнес-цілі
- Визначити технічний обсяг активів і компонентів

- Створити декомпозиція програми та визначити елементи керування програмою
- Проаналізувати загрози
- Виявити вразливостей
- Змоделювати атаки
- Створити оцінку ризиків і розробити контрзаходів

Visual, Agile, and Simple Threat (VAST) - це автоматизований метод моделювання загроз, побудований на платформі ThreatModeler. Великі підприємства впроваджують VAST у всій своїй інфраструктурі, щоб отримувати надійні, ефективні результати та підтримувати масштабованість. VAST може інтегруватися в життєвий цикл DevOps і допомогти командам визначити різні інфраструктурні та операційні проблеми. Впровадження VAST вимагає створення двох типів моделей загроз:

- Модель загрози програми - використовує діаграму процесу для представлення архітектурного аспекту загрози
- Модель операційної загрози - використовує діаграму потоку даних для представлення загрози з точки зору зловмисника

Trike - це структура аудиту безпеки для управління ризиками та захисту за допомогою методів моделювання загроз. Trike створює покрокову матрицю зі стовпцями, що представляють загроз, і рядками, що представляють зловмисників. Кожна комірка матриці має чотири частини для відповідності можливим діям (створення, читання, оновлення та видалення) і дерево правил - визначає, дозволена, заборонена або дозволена дія за допомогою правил. Trike створює діаграму потоку даних, що відображає кожен елемент у відповідних активах і акторах із визначеними вимогами. Trike оцінює ризики атаки за допомогою п’ятибальної шкали ймовірності для кожної дії.

Attack Trees - це діаграми, які відображають шляхи, якими можуть пройти атаки в системі. Ці діаграми відображають цілі атаки як корінь з можливими

шляхами - як гілки. Під час створення дерев для моделювання загроз для однієї системи створюється кілька дерев, по одному для кожної цілі зловмисника. Це один із найстаріших і найпоширеніших методів моделювання загроз. Цей тип підходу часто включається як частина внутрішніх перевірок потоку даних під час вивчення ризику постачальника та сумісності таких систем, як веб, CRM, серверні дані тощо. Хоча колись він використовувався окремо, зараз його часто поєднують з іншими методологіями, включаючи PASTA і STRIDE.

Переваги використання методів моделювання

Раннє виявлення потенційних проблем - виявивши потенційні загрози та вразливі місця на етапі проектування, організації можуть уникнути дорогих і трудомістких виправлень пізніше в процесі розробки. Цей проактивний підхід дозволяє організаціям із самого початку створювати засоби безпеки у своїх системах, а не намагатися налагоджувати їх на задній план. Раннє виявлення потенційних проблем також дає розробникам можливість вирішити їх у своєму коді. Це може призвести до більш безпечного програмного забезпечення та може допомогти уникнути потреби в дорогих і руйнівних виправленнях або оновленнях пізніше. По суті, моделювання загроз може допомогти перетворити безпеку на проактивний процес.

Розуміючи потенційні загрози для системи та вплив, який можуть мати збої в підтримці належного стану безпеки, організації можуть визначити, які засоби контролю безпеки їм потрібно запровадити, щоб захистити свої активи. Ці вимоги безпеки повинні бути включені в процес проектування та розробки системи, гарантуючи, що система побудована з урахуванням безпеки з самого початку. Це може привести до більш безпечних систем і може допомогти організаціям уникнути дорогих і руйнівних порушень безпеки. Однак, оскільки безпека часто залишається позаду, створення ліній зв’язку між IT, безпекою та розробкою є ключовою вимогою для безперервності бізнесу та побудови сценарію аварійного відновлення.

Створивши детальну модель основних елементів найважливіших бізнес-систем у всій організації, керівництво безпеки та групи ризиків можуть отримати краще розуміння того, що їм потрібно захищати, хто може атакувати це та як вони можуть це захистити. Наприклад, якщо бізнес є транзакційним веб-сайтом, розміщення елементів керування навколо веб-інтерфейсу, API та внутрішніх баз даних має бути пріоритетним. Для підприємства, що займається виробництвом, підтримання облікових записів обслуговування та ICS у належному стані та обмеження будь-якого зовнішнього доступу може бути першочерговим.

Таке розуміння може допомогти організаціям визначити пріоритети своїх зусиль і ресурсів безпеки, зосередившись на найбільш критичних активах і загрозах. Він також може надати чітку дорожню карту для впровадження заходів безпеки, допомагаючи організаціям забезпечити ефективний захист своїх систем і даних.

Методи оцінки загроз

Оцінка загрози – це інструмент, який використовують правоохоронні органи, державні органи, промисловість і більшість спеціалістів із безпеки. Це можуть бути дуже детальні та вичерпні письмові документи або просто усвідомлення потенційних загроз, з якими стикаються в різних ситуаціях. Охоронці можуть використовувати цю інформацію на початку виконання своїх обов'язків.

Наступним кроком у оцінці загрози є вивчення ризиків. У цьому розділі не буду вдаватися в подробиці, але слід розуміти, що після виявлення загрози вкрай важливо, щоб співробітники розуміли ризики, пов’язані з цією конкретною загрозою.

Методи можна поділити на два типи: якісні і кількісні. Якісні методи оцінки загроз базуються на експертній думці та якісному аналізі ризиків. Вони використовують описові та категоричні дані для оцінки загроз, до найбільш популярних якісних методів можна віднести: SWOT-аналіз, когнітивне картування, аналіз ієрархій.

Переваги якісних методів включають легкість використання, гнучкість і можливість врахування багатьох факторів, що важко кількісно виміряти. Однак, вони можуть бути суб'єктивними і менш точними.

Кількісні методи оцінки загроз базуються на числових даних і математичних моделях для визначення рівня ризику, до них можна віднести: DREAD, аналіз частоти і симуляції, Монте-Карло симуляції.

Переваги кількісних методів включають точність, об'єктивність і можливість проведення детального аналізу ризиків. Вони також дозволяють створювати математичні моделі для прогнозування і управління ризиками. Однак, їх реалізація може вимагати значних ресурсів і наявності великої кількості даних.

1.5 Порівняння методів

Переваги моделі PASTA

- Гнучкі та адаптовані - методологія, яку можна налаштувати відповідно до конкретних потреб різних організацій.
- Комплексний підхід - охоплює всі фази життєвого циклу розробки програмного забезпечення, від етапу збору вимог до обслуговування після випуску, що забезпечує комплексний підхід до моделювання загроз.
- Орієнтований на бізнес - враховує бізнес-контекст і цілі програмного додатку, гарантуючи, що модель загроз узгоджується з бізнес-цілями.
- Використовує реальні сценарії атак, що робить його більш актуальним і корисним для виявлення потенційних загроз і вразливостей.
- Ітеративна методологія, що означає, що це безперервний процес, який можна вдосконалювати та покращувати з часом на основі нової інформації та змін у програмному забезпеченні.

Недоліки моделі PASTA

- Процес може займати багато часу, особливо для більших і складніших програмних програм, які можуть потребувати більше ресурсів для завершення процесу моделювання загроз.
- Дорогий - особливо якщо організаціям потрібно найняти зовнішніх консультантів або експертів з безпеки для проведення процесу моделювання загроз.
- Ресурсовитратність - потребує залучення багатьох зацікавлених сторін, включаючи команди бізнесу, розробки та безпеки, що може бути ресурсомістким і може потребувати значної координації.
- Обмежено технічними загрозами, в основному зосереджується на технічних загрозах, таких як уразливості та експлойти, і може не розглядати інші типи загроз, такі як атаки соціальної інженерії чи внутрішні загрози.
- Може пропустити нові загрози, оскільки базується на попередніх сценаріях атак і може не враховувати нові загрози або нові вектори атак, які ще не ідентифіковані.
- Може призвести до надмірного проектування, оскільки групи безпеки можуть зосередитися на усуненні всіх потенційних загроз і вразливостей, що не завжди може бути практичним або економічно ефективним.

Переваги моделі TRIKE

- Пропонує структурований підхід, систематизуючи процес виявлення та визначення пріоритетів потенційних загроз безпеці. У результаті організації можуть зосередити свої зусилля на найбільш критичних проблемах і вразливостях.
- Поглиблений аналіз, який вона виконує на певній вразливості або зменшує масштабу, щоб побачити загальну картину, залежно від їхніх

потреб. Поєднуючи вимоги та моделі впровадження, модель TRIKE дає підприємствам повну картину свого IT-середовища.

Недоліки моделі TRIKE

- Складний у розумінні особливо для новачків у сфері кібербезпеки. Метод вимагає глибоких знань у галузі управління ризиками та аналізу загроз.
- Високі вимоги до ресурсів - може вимагати значних ресурсів, включаючи час та зусилля для побудови і підтримки моделі загроз
- Складність інтеграції - це може обмежити його застосування у більш комплексних системах або великих організаціях.

Переваги моделі VAST

- Чітка візуалізація - використовує діаграми, які чітко представляють загрози та засоби пом’якшення, допомагаючи командам швидко зрозуміти стан безпеки системи.
- VAST розроблено таким чином, щоб добре вписуватися в гнучкі фреймворки, забезпечуючи безперервне та ітераційне моделювання загроз як частину процесу розробки.
- Часто використовує автоматизовані інструменти, які можуть оптимізувати процес моделювання загроз і забезпечити узгодженість у виявленні та пом’якшенні загроз.

Недоліки моделі VAST

- Командам може знадобитися час, щоб ознайомитися з моделлю VAST та її інструментами, що вимагає початкових інвестицій у навчання та налаштування

- Ефективність може значною мірою залежати від використовуваних інструментів, і може бути недостатньо гнучкості, якщо ці інструменти не відповідають конкретним потребам проєкту.
- Безперервний цикл моделі може призвести до більшого споживання ресурсів як з точки зору часу, так і обчислювальної потужності, що може не підійти для менших проектів.
- Можуть знадобитися різні налаштування відповідно до конкретних потреб різних проектів, що може збільшити початковий час і зусилля на реалізацію.

Переваги моделі Attack Trees

- Деревоподібна структура дозволяє розбивати складні атаки на менші, більш керовані підатаки, що полегшує детальний аналіз кожної частини.
- Організації можуть визначити та усунути основні причини вразливостей, відслідкувавши їх перше джерело
- Може допомогти визначити пріоритетність загроз на основі їхньої ймовірності та впливу, сприяючи ефективному управлінню ризиками.
- Може бути налаштована відповідно до різних систем, середовищ і сценаріїв загроз, що робить їх універсальними для різних програм.

Недоліки моделі Attack Trees

- Розробка моделі може зайняти багато часу, особливо для складних систем.
- Ефективність дерев атаки залежить від досвіду людей, які їх створюють, тобто неправильні оцінки можуть призвести до неповних або неточних моделей загроз.
- Бракує стандартизованих інструментів і документацій по роботі з методом

Маючи детальний розбір кожної методології, я склала таблицю порівнянь до кожних методів з урахуванням критеріїв для вибору найбільш релевантної методології

Таблиця 1.1 – Порівняльна таблиця методологій

Критерій	**STRIDE**	**PASTA**	**VAST**	**TRIKE**	**Attack Trees**
Гнучкість у використані	+	-складний для адаптацій	+	-складний у використані	+
Підходить для великих систем	+	+	-, підходить тільки для невеликих	+	+
Підходить для великих систем	+	+	-, підходить тільки для невеликих	+	+
Складність реалізації	-, реалізувати просто	+	-, реалізувати просто	+	-, реалізувати просто
Застосовуєтьс я до різних типів загроз	+	+	-, є тільки певний тип	+	+
Інтеграція з іншими методами	+	-, важко інтегрувати	+	-, важко інтегрувати	+
Зручність у використанні	+	-, потребує багато ресурів	+	-, потребує глибоких знань	+

Враховуючи всі можливості методологій та їх плюси, на мою думку, найкраща в реалізація є методологія STRIDE, саме тому я її використала в своїй роботі.

Висновки до розділу 1

CRM – це потужний інструмент для збереження та обробки даних. Оскільки CRM-системи обробляють велику кількість конфіденційних даних, безпека цих систем є критично важливою для запобігання витоку інформації та захисту бізнесу. Потрібно зважати на всі можливі загрози та які наслідки це матиме для користувачів та бізнесу. Моделювання та оцінка загроз є важливими етапами в забезпеченні інформаційної безпеки CRM-систем. Впровадження моделюваня загроз допомагає ідентифікувати потейні загрози, які можуть бути як і внутрішніми, так і зовнішніми та використовуватись для компроментації даних. Завдяки фінальній моделі можливо прогнозувати майбутні сценраії атак та створювати найкращі заходи захисту спираючись на готову модель загроз.

Оцінка загроз допомагає визначити найбільш критичну загрозу ти наскільки сильним може бути ризик. Також, після проведення оцінювання з легкістю можна визначити пріорітетні заходи безпеки для оптимального розподілення ресурсів захисту і розуміння, які додаткові сили мають бути залучені для отримання необіхдного рівня захисту.

2 МОДЕЛЬ ЗАГРОЗ CRM-СИСТЕМИ НА ОСНОВІ МЕТОДОЛОГІЇ STRIDE

Модель загроз CRM-системи на основі методології STRIDE допомагає виявляти та аналізувати потенційні ризики, які можуть виникнути в процесі використання CRM. Це важливо для того, щоб уникнути можливих проблем і забезпечити безпеку та надійність роботи системи. Такий підхід дозволяє компаніям розробляти ефективні стратегії захисту та вчасно реагувати на потенційні загрози, що дозволяє зберігати високий рівень довіри користувачів і підтримувати ефективну роботу бізнесу.

2.1 Переваги використання методології

Перевага STRIDE полягає в тому, що він дозволяє організаціям аналізувати системи та мережі, класифікуючи загрози в пріоритетному списку на основі ймовірності їх виникнення та масштабу їх потенційного впливу.

Наприклад, організація охорони здоров’я, яка використовує STRIDE, може розглядати конфіденційність інформації про пацієнта як головний пріоритет безпеки, ризикуючи розголошенням конфіденційних даних або несанкціонованим доступом. Підвищуючи ці загрози як потенційно серйозні, організація може розробити та впровадити контрзаходи, які будуть ефективними для запобігання цьому. Ця методологія особливо корисна для компаній, які мають чітке розуміння загроз і вразливостей, з якими вони стикаються

Переван використання STRIDE є безліч. Опишу, які я виділила основними:

Цілісний підхід

STRIDE охоплює широкий спектр загроз безпеці, зосереджуючись на шести різних категоріях. Цей комплексний підхід забезпечує врахування всіх значущих типів загроз, зменшуючи ймовірність того, що критичні вразливості будуть пропущені. Кожна категорія в STRIDE націлена на певний аспект безпеки, що дозволяє ретельно вивчити потенційні вразливості. Наприклад, підробка зосереджена на проблемах ідентифікації, тоді як втручання вирішує цілісність даних, забезпечуючи ретельну перевірку кожного аспекту безпеки.

Структурована та систематична методологія

Структурований характер STRIDE забезпечує чітку структуру для виявлення та усунення загроз. Цей системний підхід допомагає переконатися, що процес моделювання загроз є ретельним і методичним, зменшуючи ймовірність пропуску важливих вразливостей. Покрокова методологія STRIDE дозволяє фахівцям із безпеки методично оцінювати кожен компонент системи щодо кожної категорії загроз, забезпечуючи комплексну оцінку безпеки.

Простота інтеграції

STRIDE можна легко інтегрувати в різні методології розробки, включаючи Agile та DevOps. Ця сумісність гарантує, що питання безпеки враховуються протягом усього життєвого циклу розробки, від проектування до розгортання. Завдяки інтеграції STRIDE на ранніх етапах розробки потенційні загрози можна виявити та пом’якшити до того, як вони стануть серйозними. Цей проактивний підхід допомагає зменшити вартість і складність усунення вразливостей безпеки на пізнішому етапі процесу розробки.

Чітка документація

Структурований характер STRIDE сприяє чіткому та послідовному документуванню виявлених загроз та засобів пом’якшення. Ця документація є

цінною для майбутніх довідок, аудиту та відповідності, а також для залучення нових членів команди

Адаптація під нові загрози

Гнучкість STRIDE дозволяє адаптуватися до нових загроз і мінливого середовища безпеки. Використовуючи найновішу інформацію про загрози, організації можуть гарантувати, що їхні заходи безпеки залишатимуться ефективними та актуальними. STRIDE підтримує постійну оцінку безпеки протягом життєвого циклу розробки. Регулярний перегляд і оновлення моделі загроз гарантує виявлення нових загроз і їх усунення в міру розвитку системи

Для виконання завдання компанія “AIM” надала мені доступ до своєї власної CRM-системи, для неї я створювала модель загроз та оцінку існуючих ризиків. Щоб визначити основні компоненти, які піддатливі загрозам я побудувала діаграму потоку даних, за допомогою ПЗ Microsoft

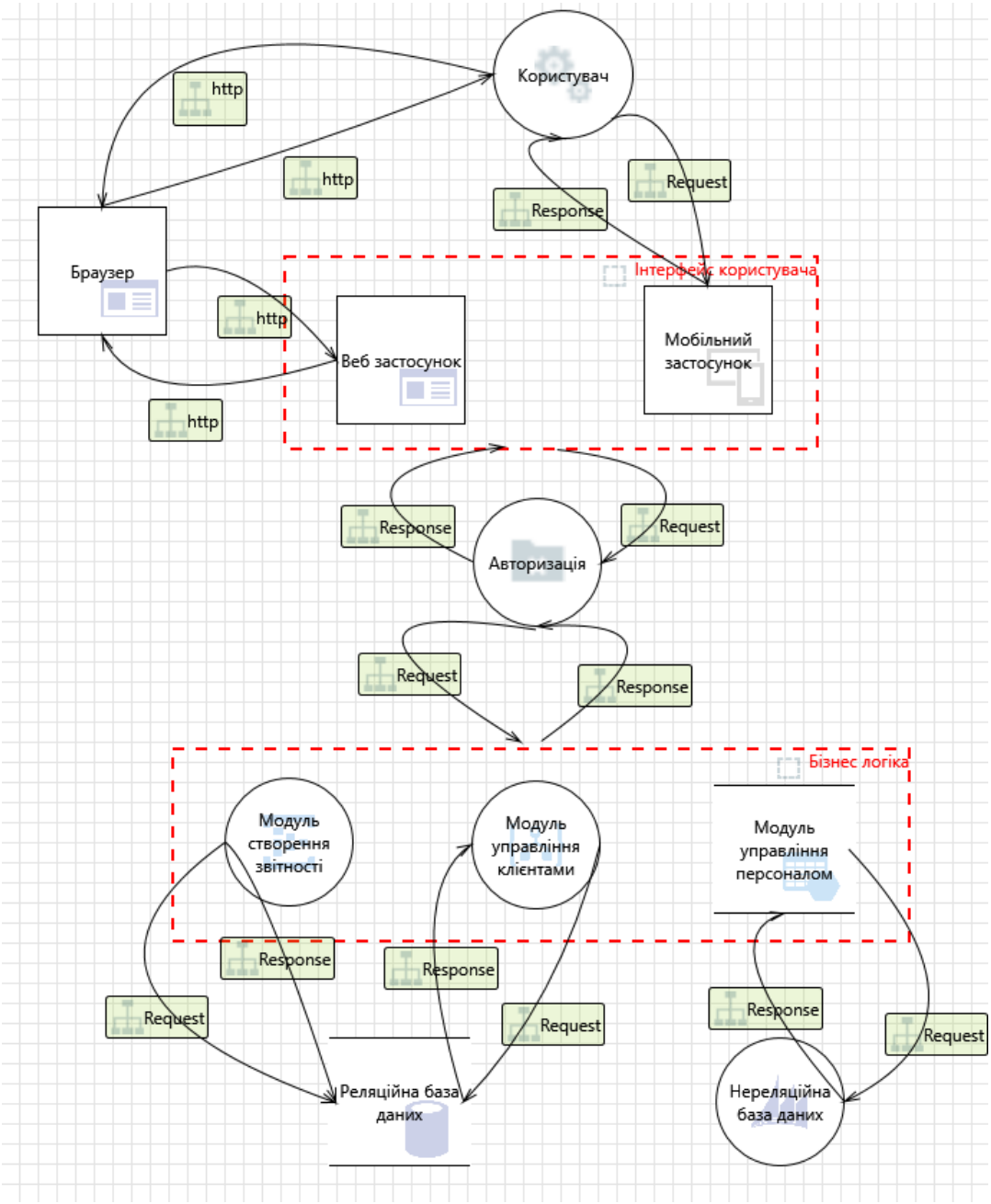

Рисунок 2.1 – Діаграма потоку даних

2.2 Визначення загроз

Маючи зображення потоку даних можна побудувати модель загроз для кожного компоненту спираючись на результати та виявлені загрози ПЗ Microsoft.

Використовуючи методологію STRIDE, були побудовані наступні модель загроз для системи:

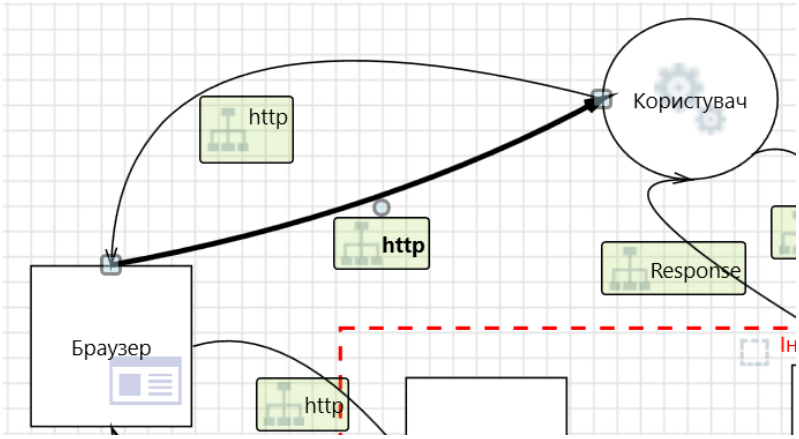

Рисунок 2.2 – Взаємодія компонентів користувач та браузер

Таблиця 2.1 – Модель загроз компонентів користувач та браузер

Ризик	**Загроза**	**Метод запобігання**	**Стадія розробки**
Spoofing	Підробка користувача	обмеження доступу за IP-адресами	-
Tampering	Підробка даних між клієнтом і сервером	Використання HTTPS для шифрування даних	-
Information Disclosure	Перехоплення нешифрованих даних під час передачі	GDPR	-

Компоненти браузер та веб застосунок

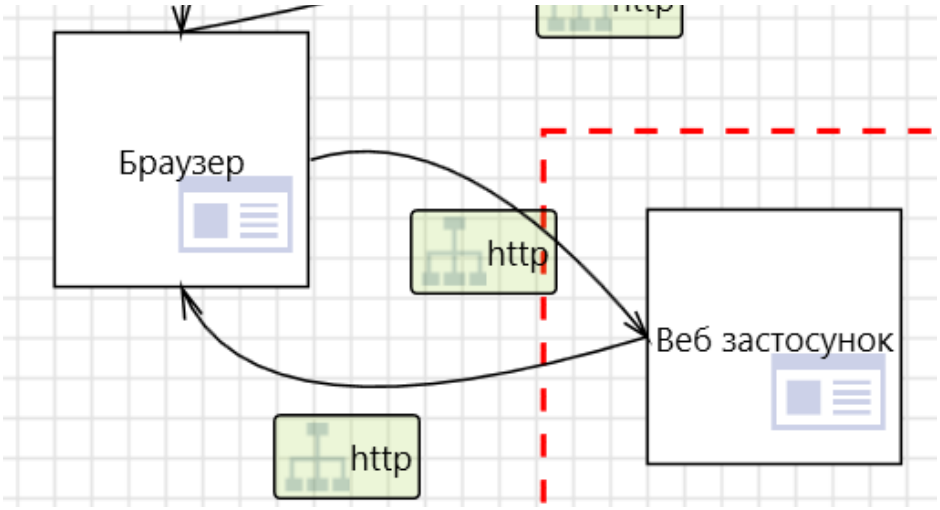

Рисунок 2.3 - Взаємодія компонентів браузер веб застосунок

Таблиця 2.2 - Модель загроз компонентів браузер веб застосунок

Ризик	**Загроза**	**Метод запобігання**	**Стадія розробки**
Spoofing	Підробка користувача	обмеження доступу за IP-адресами	проектування
Tampering	Підробка даних між клієнтом і сервером	Використання HTTPS для шифрування даних	проектування
Information Disclosure	Перехоплення нешифрованих даних під час передачі	GDPR	проектування
DoS	Система стає недоступною для легітимних користувачів	Обмеження швидкості запитів	Тест системи

Компоненти користувач та мобільний застосунок

Рисунок 2.4 - Взаємодія компонентів браузер веб застосунок

Таблиця 2.3 - Модель загроз компонентів браузер веб застосунок

Ризик	**Загроза**	**Метод запобігання**	**Стадія розробки**
Spoofing	Підробка користувача	обмеження доступу за IP-адресами	проектування
Tampering	Підробка даних між клієнтом і сервером	Використання HTTPS для шифрування даних	проектування
Information Disclosure	Перехоплення нешифрованих даних під час передачі	GDPR	проектування

Кінець таблиці 2.3

DoS	Система стає недоступною для легітимних користувачів	Обмеження швидкості запитів	Тест системи

Компоненти інтерфейс користувача та авторизація

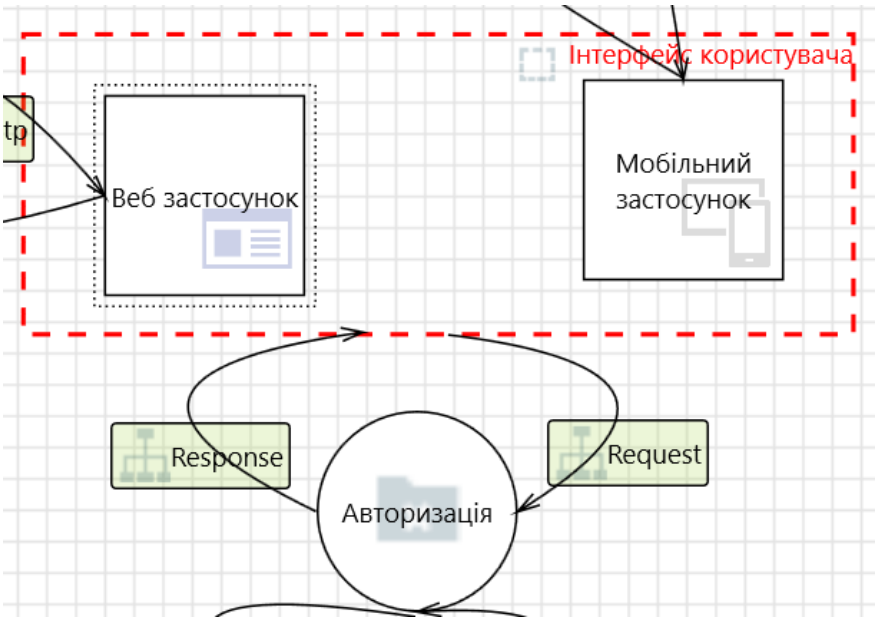

Рисунок 2.5 - Взаємодія компонентів інтерфейс користувача та авторизація

Таблиця 2.4 - Модель загроз компонентів інтерфейс користувача та авторизація

Ризик	**Загроза**	**Метод запобігання**	**Стадія розробки**
Spoofing	Фішингові атаки для отримання облікових даних користувачів.	MFA, Періодичне оновлення даних для авторизації	Тестування системи

Кінець таблиці 2.4

Tampering	Перехоплення та зміна даних у процесі передачі.	Використання HTTPS для шифрування даних	Впровадження системи
Information Disclosure	Витік конфіденційної інформації через інтерфейс користувача або процес авторизації.	HTTPS	проектування
DoS	Система стає недоступною через навмисні дії зловмисників, спрямовані на інтерфейс користувача або процес авторизації	Введення тимчасового блокування після кількох невдалих спроб входу.	Впровадження системи
Repudiation	Користувач стверджує, що не здійснював певних дій, записаних у системі	Ведення детальних журналів (логів) активності	Проектування

Компоненти авторизація та бізнес-логіка

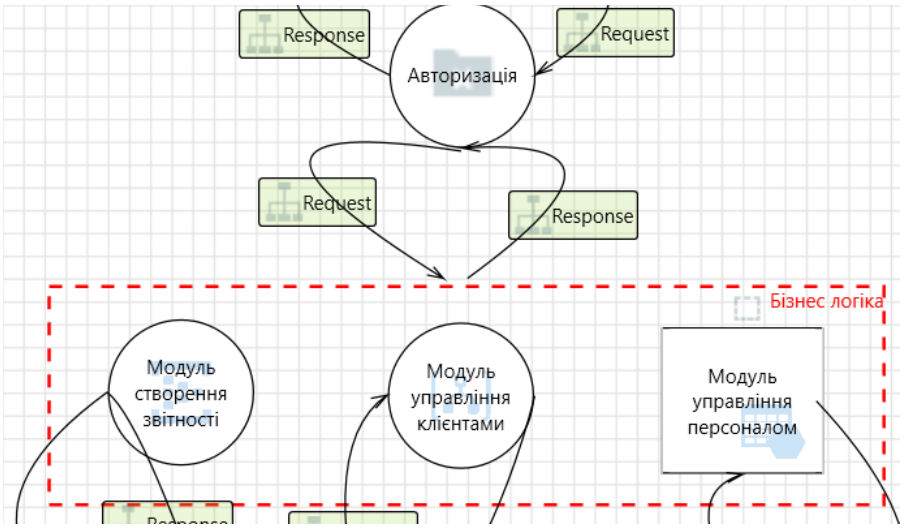

Рисунок 2.6 - Взаємодія компонентів авторизація та бізнес-логіка

Таблиця 2.5 - Модель загроз компонентів авторизація та бізнес-логіка

Ризик	**Загроза**	**Метод запобігання**	**Стадія розробки**
Elevation of Privileges	Користувач отримує вищі права доступу через виконання певних дій у системі	Регулярний аудит прав доступу	Впровадження
Information Disclosure	Несанкціонований доступ до конфіденційної інформації	Політика управління доступом	Впровадження
Elevation of Privileges	Неправильна конфігурація ролей безпеки	Політика управління доступом	Проектування

Кінець таблиці 2.5

DoS	Система стає недоступною через навмисні дії зловмисників	Nist	Впровадження

Компоненти модуль створення звітності та реляційна база даних

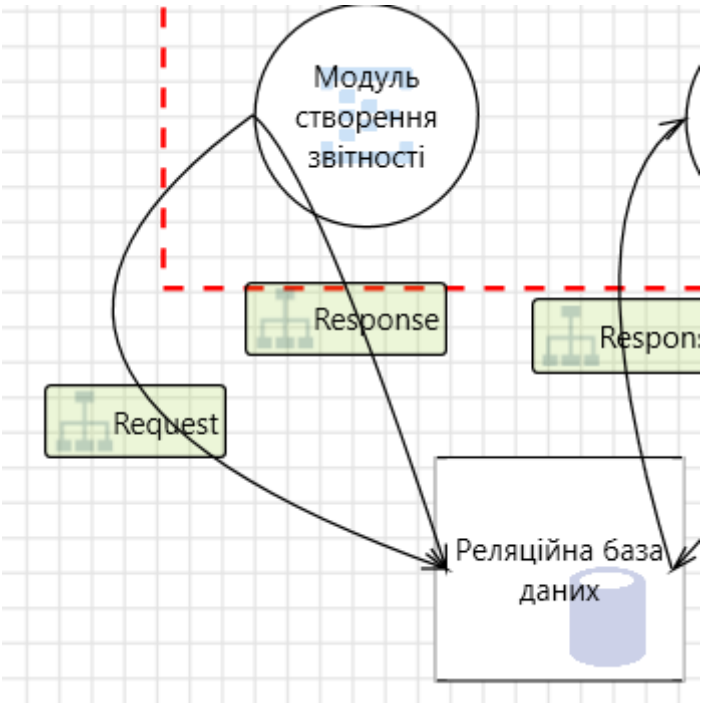

Рисунок 2.7 - Взаємодія компонентів модуль створення звітності та реляційна база даних

Таблиця 2.6 - Модель загроз компонентів модуль створення звітності та реляційна база даних

Ризик	**Загроза**	**Метод запобігання**	**Стадія розробки**
Information Disclosure	Витік даних	Шифрування даних	Імплементація БД

Кінець таблиці 2.6

Information Disclosure	Незахищені дані звітів можуть бути розкриті несанкціонованим користувачам	Політика управління доступом	Імплементація БД
Elevation of Privileges	Неправильна конфігурація ролей безпеки	Політика управління доступом	Проектування
Repudiation	Відсутність надійних механізмів логування та аудиту	MFA	Впровадження
Tampering	Зловмисник може змінити або підробити дані, які використовуються для створення звітів, або самі звіти	Ведення журналів (логів) змін даних і створених звітів	Впровадження

Компоненти модуль створення звітності та реляційна база даних

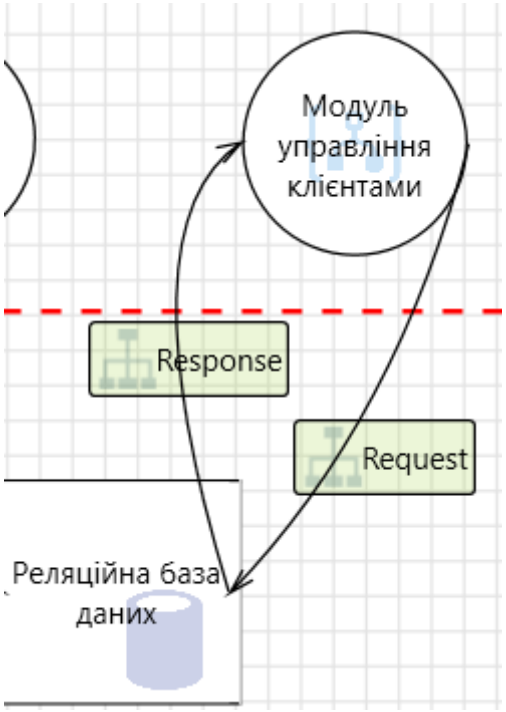

Рисунок 2.8 - Взаємодія компонентів модуль управління клієнтами та реляційна база даних

Таблиця 2.7 - Модель загроз компонентів модуль управління клієнтами та реляційна база даних

Spoofing	Зловмисник може підробити ідентичність користувача	Обмеження доступу за IP-адресою	Впровадження системи
Information Disclosure	Незахищені дані клієнтів можуть бути розкриті несанкціонованим користувачам	Шифрування даних	проектування

Кінець таблиці 2.7

Information Disclosure	Неправильні налаштування доступу до бази даних клієнтів	Використання механізмів авторизації для перевірки прав доступу	Впровадження системи
Tampering	Зловмисник може змінити або підробити дані клієнтів у базі даних	Обмеження прав доступу відповідно до принципу найменших привілеїв.	Проектування
Elevation of Privilege	Використання вразливостей для отримання адміністративних прав	Регулярний аудит прав доступу	Тестування

Компоненти модуль створення звітності та реляційна база даних

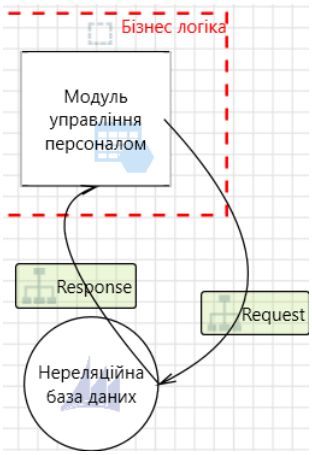

Рисунок 2.9 - Взаємодія компонентів модуль управління персоналом та нереляційна база даних

Таблиця 2.8 - Модель загроз компонентів модуль управління персоналом та нереляційна база даних

Information Disclosure	Незахищені дані звітів можуть бути розкриті несанкціонованим користувачам	Політика управління доступом	Імплементація БД
Information Disclosure	Ображені працівники можуть змінити або видалити дані	Політика управління доступом	Імплементація БД
Information Disclosure	Інформація може загубитись в великій кількості даних	Аудит журналів	Імплементація БД
Elevation of Privileges	Неправильна конфігурація ролей безпеки	Політика управління доступом	Проектування
Repudiation	Відсутність надійних механізмів логування та аудиту	MFA	Впровадження
Tampering	Зловмисник може змінити або підробити дані	Ведення журналів (логів) змін даних і створених звітів	Впровадження

Відносно проведеного аналізу загроз, можна скласти модель загроз вцілому для CRM та виділити, які з них є найбільш критичними і мають найбільш вплив у разі їх реалізації. Дані загрози наведені у таблиці 2.9

Таблиця 2.9 – Модель загроз для CRM

Ризик	**Загроза**	**Наслідки**	**Компонент**
Spoofing	Можливість підробки інтерфейсу	Витік інформації, зупинка роботи системи	Інтерфейс користувача
Tampering	Несанкціонована зміна даних	Втрата даних або порушення цілісності	Бази даних
Repudiation	Відсутність надійних механізмів логування та аудиту	Складнощів у виявленні та підтвердженні дій користувачів	Користувач
Information Disclosure	Несанкціонований доступ до конфіденційної інформації	Розголошення інформації	Бази даних, авторизація
DoS	Атаки на CRM сервер	Перевантаження та відмова в обслуговуванні користувачів	Веб застосунок, мобільний застосунок
Elevation of Privilege	Несанкціоноване підвищення рівня доступу до даних або функцій	Порушення конфіденційності або цілісності інформації	Бази даних, Користувач, авторизація

Зображення конкретно цих загроз було здійснене на підставі найбільш ймовірних негаразд з системою та тих, які вже траплялись в минулому. Отже, з таблиці можна виділити, що найбільш критичного збитку загрози будуть наности для баз даних.

2.3 Оцінка загроз

Для визначення впливовості загрози та оцінки її наслідків, проводиться якісний і кількісний аналіз. Під час якісного аналізу визначається ранг загрози і ймовірність її виникнення.

Знаючи, які загрози є потенційними та, які компоненти є найбільш вразливими, я можу побудувати повноцінну когнітивну модель. Також варто звертати увагу на внутрішню взаємодію загроз, оскільки реалізація однієї загрози може вплинути на реалізацію іншої, потрібно враховувати їх зв'язки та впливовість.

Для початку побудови моделі, потрібно визначити ранжування ризиків, отриманий реєстр – таблиця 3.2, допоможе з побудовою матриці взаємозв’язків, яка в подальшому буде використовуватись для визначення найбільшої загрози і пропозицій, як це можна вирішити

Таблиця 2.10 – Оцінювання загроз системи

ID	Загроза	P	L	R
K1	Можливість підробки інтерфейсу	0,05	0,1	0,005
K2	Несанкціонована зміна даних	0,4	0,3	0,12
K3	Відсутність надійних механізмів логування та аудиту	0,3	0,1	0,03
K4	Несанкціонований доступ до конфіденційної інформації	0,6	0,4	0,24
K5	Атаки на CRM сервер	0,2	0,5	0,1
K6	Несанкціоноване підвищення рівня доступу до даних або функцій	0,1	0,6	0,06

Цей метод оцінювання є якісним, тому для визначення P (ймовірність виникнення), L (ступінь впливу), R (ранг загрози) – використовувався метод експертних оцінок, а саме фахівців ІТ-відділу компанії AIM. R визначався за формулою:

$$R = P*L$$

Розглянувши отримані результати, можна стверджувати, що найбільшого збитку може нанести загроза К4- несанкціонований доступ до конфіденційної інформації. Отримані значення є основою для побудови когнітивної карти рис.3.2, яка являється орієнтованим графом, що відображує взаємозв'язки між загрозами.

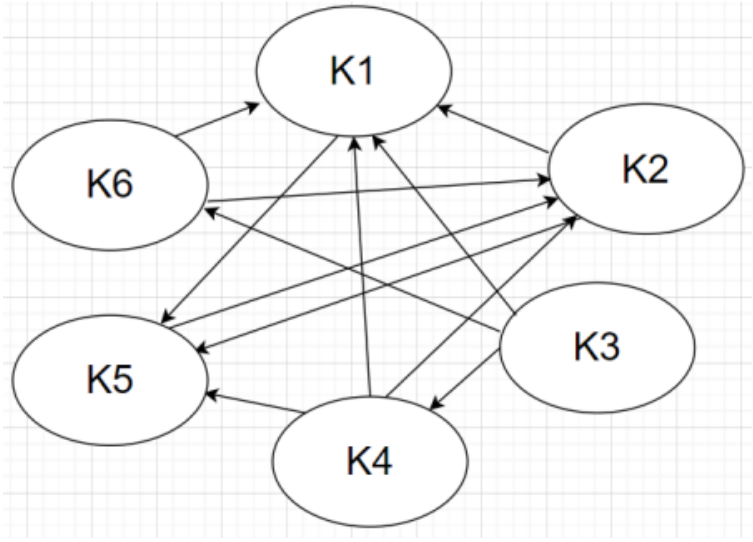

Рисунок 2.10 – Когнітивна карта загроз

Для розширення когнітивної карти потрібно представити більш детальну інформацію про взаємозв'язки між ризиками, так за допомогою методу експертного оцінювання фахівцями, спираючись на попередньо створене ранжування загроз була створена таблиця 3.3

Таблиця 2.11 – Матриця взаємозв'язків загроз з коефіцієнтами впливу

	К1	**К2**	**К3**	**К4**	**К5**	**К6**
К1	0	0	0	0	0,85	0
К2	0,15	0	0	0	0,6	0
К3	0,35	0	0	0,5	0	0,6

Кінець таблиці 2.11

К4	0,15	0,85	0	0	1	0
К5	0	0,35	0	0	0	0
К6	0,16	0,6	0	0	0	0

Представлені у таблиці цифри визначались за нечіткою лінгвістичною шкалою, де сила зв'язку має свої відповідні значення рис. 2.11

Рисунок 2.11 – Шкала сили зв’язку

З цієї матриці можна визначити, що найбільший вплив на систему має загроза К4, а саме несанкціонований доступ до конфіденційної інформації, це може призвести до злому системи і загальної зупинки роботи серверу, що понесе за собою великі втрати компанії. Порівнюючі отриманний результат з таблицею 2.10 , можна підтвердити, що дійсно загроза К4 є найбільш значуща.

Провівши усі обрахунки по оцінці загроз, можна стверджувати, що конгітивне картування є доцільним застосуванням під час робробки моделі загроз для того, щоб прорахувати на скільки сильний вплив вони можуть

Висновки до розділу 2

Моделювання загроз STRIDE пропонує надійний і систематичний підхід до виявлення та пом’якшення загроз безпеці. Його повне охоплення, структурована методологія, легкість інтеграції та підтримка чіткого зв’язку роблять його цінним інструментом для підвищення безпеки систем і програм. Забезпечуючи раннє виявлення та визначення пріоритетів загроз, STRIDE допомагає організаціям ефективно керувати ризиками, гарантуючи, що питання безпеки є невід’ємною частиною життєвого циклу розробки. За допомогою ПЗ Microsoft Threat Modelling Tool, була побудована наступна діаграма потоку даних

3 МЕТОДИ ПІДВИЩЕННЯ ЗАХИЩЕННОСТІ CRM-СИСТЕМИ

Методи підвищення захисту CRM системи включають в себе широкий спектр стратегій та практик, спрямованих на забезпечення надійності та безпеки системи в умовах постійно зростаючих кіберзагроз. Застосування моделі для визначення зрілості компанії відносно кіберзагроз є важливим етапом у підвищенні захищенності CRM системи. Ця модель дозволяє оцінювати рівень готовності компанії до різних видів кіберзагроз, ідентифікувати слабкі місця та розробляти стратегії захисту, які враховують конкретні потреби та можливості компанії.

Програмна реалізація моделі для визначення зрілості компанії відносно кіберзагроз є ключовим кроком у впровадженні заходів підвищення захисту CRM системи. Це включає в себе розробку спеціалізованого програмного забезпечення для збору та аналізу даних про кіберзагрози, автоматизацію процесів оцінки ризиків та впровадження превентивних заходів захисту.

У контексті пропозицій підвищення захищеності систем CRM, важливо враховувати не лише технічні аспекти, але й організаційні та людські чинники. Наприклад, проведення регулярних навчань та тренувань з безпеки для персоналу, впровадження мультифакторної аутентифікації, а також постійний моніторинг та аналіз кіберзагроз можуть значно підвищити рівень захисту CRM системи.

Таким чином, ефективне поєднання технічних, організаційних та навчальних заходів дозволяє створити комплексний підхід до захисту CRM системи від сучасних кіберзагроз.

3.1 Модель визначення зрілості компанії відносно кіберзагроз

Оцінка зрілості компанії щодо кіберзагроз є важливим етапом у забезпеченні безпеки не тільки CRM-системи, а й всієї компанії . Це дозволяє виявити слабкі місця, оцінити поточний стан безпеки і розробити план для вдосконалення. Застосування моделі STRIDE визначає загрози, але щоб дізнатись рівень захищенності, необхідно порівняти, на яких етапах – табл. 3.4 можливі впроваджені етапи захисту системи

Таблиця 3.1 –Рівні зрілості компанії на основі впровадженої CRM

Етап	**Його опис**
Оцінка захисту технічними засобами	Включає оцінку впровадження технічних засобів захисту, які використовуються компанією
Оцінка процесів та політик безпеки	Аналіз існуючих процесів та політик безпеки відносно найбільшої загрози
Оцінка рівня обізнаності та підготовки співробітників щодо кіберзагроз і методів захисту	Цей етап включає в себе перевірку обізнаності персонала та їх реагування на виникнення загроз
Фінальна оцінка зрілості	Оцінка зрілості буде визначена рівнем враховуючи попередні твердження під час оцінювання

Відповідно до попередніх розрахунків та когнітивної моделі, я визначила, що найбільша загроза є К4 - несанкціонований доступ до конфіденційної інформації, тому відносно нього буде відбуватись оцінювання компанії. Для абстрактного оцінювання будуть застосовуватись цифри: “1” – засіб захисту впроваджений або компанія дотримується правл і стандартів;

“0” – компанія немає цього засобу та не дотримується стандартів

Таблиця 3.2 – Перший етап, оцінка захисту технічними засобами

Назва засобу	**Його застосування**
IDS/IPS	0
Шифрування даних	1
MFA	0
Антивірусне ПЗ	1

Таблиця 3.3 – Другий етап, оцінка процесів та політик безпеки

Назва політики	**Його застосування**
Політики управління доступом	0
Процедури управління інцидентами	1
Політика резервного копіювання	0
Застосування GDPR/NIST	0

Таблиця 3.4 – Третій етап, оцінка рівня обізнаності та підготовки співробітників щодо кіберзагроз і методів захисту

Назва заходу	**Його застосування**
Методичні матеріали по кібергігієні	1
Проведення тестування на знання дій у випадках реалізації загрози	0
Проведення тренінгів по кібербезпеці	0

Кінець таблиці 3.4

Періодичне оновлення даних для авторизації	1

Для коректної оцінки захищенності введемо поняття рівнів захищенності та відповідну шкалу оцінювання:

- Слабкий рівень захищенності – 0-4 балів
- Середній рівень захищенності – 5-7 балів
- Достатній рівень захищенності – 8-10 балів
- Високий рівень захищенності – 11-12 балів

Обрахувавши отримані дані з таблиць 3.5-3.7, я отримала результат – 5 балів, відповідно до шкали захищенності можна стверджувати, що у компанії середній рівень захищенності відносно кіберзагроз. Оскільки CRM-система компанії є найважливішою складовою функціонування бізнесу, то можна стверджувати, що нехтування впровадження систем захисту та інших критеріїв, які вказані в таблицях – призведе до серйозних наслідків. А саме, як я визначила під час оцінки та моделювання загроз, це злом системи і загальна зупинки роботи серверу, що понесе за собою великі втрати компанії та неможливість відновлення роботи, а також репутаціцйні збитки через витік інформації.

Наявність цієї моделі з подальшим її використанням для визначення захищеності компанії впливає не тільки на оцінку кіберзахищенності компанії у власних потреб, а й за допомогою цих критеріїв можливо виявити слабкі місця та скласти рекомендації щодо покращення захисту і в майбутньому уникнення усіх загроз.

3.2 Програмна реалізація моделі для визначення зрілості компанії відносно кіберзагроз

Відкриваючи програму, користувача зустрічає вікно – рис 3.4, яке пропонує оцінити зрілість компаніх

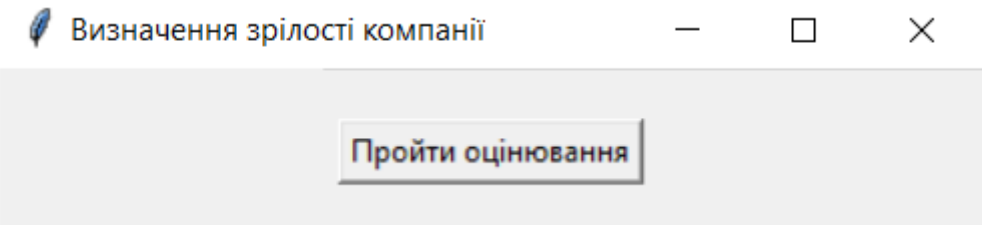

Рисунок 3.4 – Початкове вікно програми

Натискаючи на кнопку, відкривається вікно з усіма заходами – рис. 3.5, які повинні бути впроваджені для запобігання загроз, які релевантні за методології STRIDE

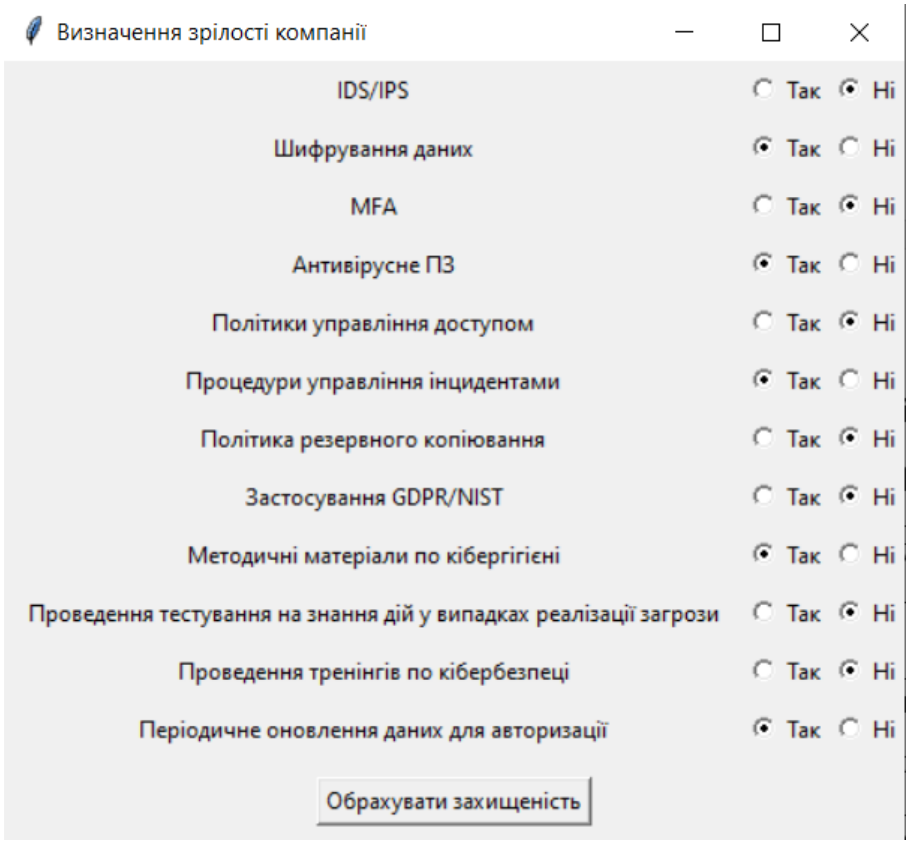

Рисунок 3.5 – Вікно з вибором застосованих заходів

Якщо цей певний захід безпеки застосовується – потрібно натиснути ‘так’ і програма зарахує це, як 1 бал, якщо не застосовується, потрібно обрати ‘ні’ і цей захід у фінальну оцінку входити не буде. Обрахунок відбувається шляхом додавання вжитих заходів та оцінюються рівень зрілості по шкалі, яка була описана в підпункті 3.3

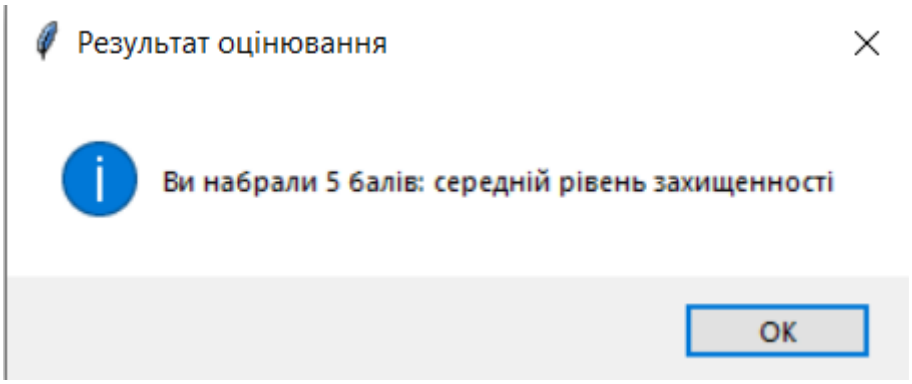

Рисунок 3.6 – Фінальний результат оцінювання

3.3Пропозиції підвищення захищенності систем

Щоб підвищити захищеність CRM-системи від визначених загроз, можна застосувати такі заходи

Можливість підробки інтерфейсу

- Використання HTTPS – це забезпечить шифрування даних, що передаються між клієнтом і сервером
- Навчання працівників – для розпізнавання підробленого інтерфейсу та для набуття навичок реагування на фішингові атаки

Несанкціонована зміна даних

- Впровадження політики доступу – це допоможе обмежити права користувачів на зміну даних
- Логування – запис всіх операцій зі зміною даних з метою подальшого аудити
- Політика резервного копіювання – у разі зміни або видалені даних це надійний метод їх відновлення

Відсутність надійних механізмів логування та аудиту

- Регулярний аудит – періодичний аналіз логів для виявлення активностей

- Політика управління інцидентами - налаштування систем оповіщення про підозрілі активності

Несанкціонований доступ до конфіденційної інформації

- MFA - використання двофакторної аутентифікації (2FA) для забезпечення безпечного доступу
- Шифрування даних - як під час передачі, так і на зберіганні, для уникнення їх викрадення або зміни
- Впровадження політик доступу - строге визначення та управління правами доступу користувачів до конфіденційної інформації.

Атаки на CRM-сервер

- IDS/IPS - використання брандмауерів та систем виявлення/запобігання вторгнень для захисту серверів
- Моніторинг - постійний моніторинг активності на сервері для виявлення та реагування на атаки.
- Застосування GDPR/NIST – для забезпечення надійного захисту серверів

Несанкціоноване підвищення рівня доступу до даних або функцій

- Періодичне оновлення даних для авторизації з метою уникнення їх витоку
- Методичні матеріали по кібергігієні – для навчання працівників базових рекомендацій, де потрібно зберігати свої дані та що з ними робити
- Контроль доступу на рівні ролей - визначення чітких ролей та обмеження прав доступу відповідно до принципу найменших привілеїв

3.4 Структура впровадження заходів безпеки

Відповідно до запропонованих заходів безпеки CRM-системи спираючись на модель, яка була визначена в розділі 2, я побудувала структуру впровадження заходів в CRM-систему рис. 3.7 для зменшення впливів загроз.

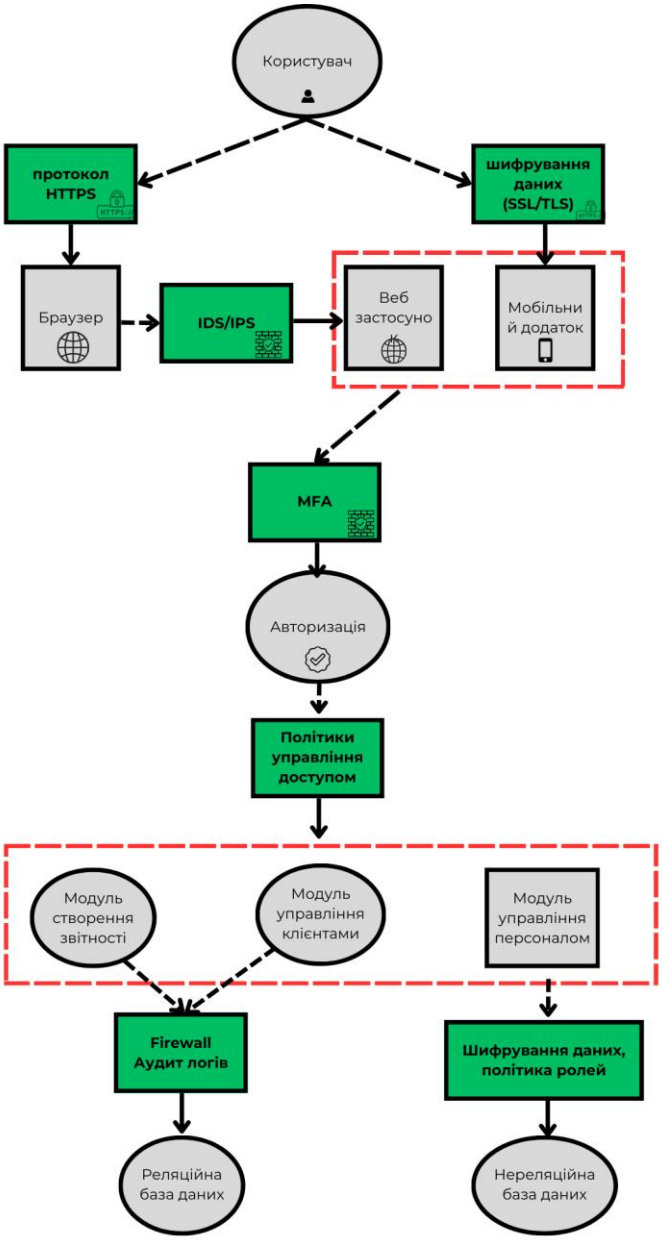

Рисунок 3.7 – Структура захисту CRM-системи

Впровадження структури захисту CRM-системи є критичним кроком для забезпечення безпеки даних клієнтів та захисту бізнесу від кіберзагроз. Захищеність CRM-системи має першорядне значення, оскільки вона містить велику кількість конфіденційної інформації, зокрема, дані клієнтів, фінансові дані, історії замовлень та інші чутливі відомості.

Одним із найважливіших заходів є шифрування даних. Шифрування даних у спокої та у транзиті забезпечує захист інформації від несанкціонованого доступу та перехоплення. Використання сильних алгоритмів шифрування, таких як AES, гарантує, що навіть у випадку компрометації системи зловмисники не зможуть прочитати або використовувати викрадені дані.

IDS дозволяє виявляти підозрілу активність у реальному часі, моніторячи мережевий трафік та системні події. IPS, в свою чергу, не тільки виявляє, але й запобігає загрозам, автоматично блокуючи шкідливу активність. Разом ці системи допомагають забезпечити безперервний моніторинг та захист від зовнішніх та внутрішніх загроз.

Багатофакторна аутентифікація (MFA) додає додатковий рівень безпеки при доступі до системи. Використання кількох факторів аутентифікації, таких як паролі, одноразові коди, біометричні дані або апаратні токени, значно ускладнює несанкціонований доступ навіть у разі компрометації одного з факторів.

Впровадження цих заходів забезпечить всебічний захист CRM-системи, мінімізуючи ризики втрати даних та забезпечуючи надійний захист від кіберзагроз. Таким чином, інвестиції у безпеку CRM-системи не лише захищають дані клієнтів, але й підтримують репутацію бізнесу та його довіру з боку клієнтів.

Висновки до розділу 3

Застосування моделі STRIDE для визначення зрілості компанії щодо кіберзагроз дозволяє систематично підходити до управління загрозами, підвищувати ефективність заходів захисту та забезпечувати безпеку CRM-системи на високому рівні. Регулярний моніторинг та аналіз загроз, а також постійне вдосконалення заходів захисту сприяють підвищенню рівня кібербезпеки та зрілості компанії в цілом

ВИСНОВКИ

У процесі зменшення ризиків для даних компанії, які зберігаються в CRM-системах, я застосувала моделювання загроз за методологією STRIDE, надає комплексний підхід до оцінки та управління загрозами. Це дозволило мені ідентифікувати основні загрози, які можуть впливати на безпеку CRM-системи, та розробити ефективну стратегію для їх усунення

У ході дослідження я визначила ключові загрози для CRM-системи. Ці загрози включають підробку інтерфейсу користувача, несанкціоновану зміну даних, відсутність надійних механізмів логування та аудиту, несанкціонований доступ до конфіденційної інформації, атаки на CRM сервер та несанкціоноване підвищення рівня доступу до даних або функцій. Кожна з цих загроз може мати значний вплив на безпеку та цілісність даних компанії, що підкреслює важливість їх ретельного аналізу та управління.

На основі визначених загроз я побудувала модель оцінки ризиків, яка дозволяє систематично оцінювати ймовірність та потенційний вплив кожної загрози на CRM-систему. Ця модель враховує різні аспекти безпеки, такі як доступність, цілісність та конфіденційність даних, а також використання сучасних технологій для забезпечення захисту. Впровадження моделі оцінки загроз допомагає не лише виявити вразливі місця системи, але й визначити найбільш ефективні заходи для їх усунення.

Далі, я створила інструмент для оцінки зрілості компанії щодо кіберзагроз на основі розробленої моделі. Цей інструмент надає можливість компаніям проводити самостійний аудит своєї CRM-системи, визначати поточний рівень безпеки та зрілості, а також отримувати рекомендації для підвищення захищеності. Інструмент включає інтерактивні елементи, які допомагають користувачам ідентифікувати слабкі місця у своїй системі та надають конкретні кроки для покращення стану кібербезпеки.

Загалом, виконана робота дозволила не лише ідентифікувати основні загрози для CRM-системи, але й розробити практичні інструменти для їх оцінки та управління. Впровадження цих рішень допоможе компаніям підвищити рівень безпеки своїх даних, забезпечити їх цілісність та конфіденційність, а також бути краще підготовленими до потенційних кіберзагроз у майбутньому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1- STRIDE – threat modelling procces. [Електронний ресурс] – Режим доступу: https://owasp.org/www-community/Threat_Modeling_Process

2- Threat Modelling – Risk Management. [Електронний ресурс] – Режим доступу: https://www.ncsc.gov.uk/collection/risk-management/threat-modelling

3 - Microsoft Security Development Lifecycle Threat Modelling. [Електронний ресурс] – Режим доступу: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

4 - How to Use the STRIDE Threat Model? . [Електронний ресурс] – Режим доступу: https://www.practical-devsecops.com/how-to-use-stride-threat-model/

5 - Value at Risk: A Methodology for Information Security Risk Assessment. [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/250719484_Value_at_Risk_A_Methodology_for_Information_Security_Risk_Assessment

6 – CRM Data Security. [Електронний ресурс] – Режим доступу: https://www.bigcontacts.com/blog/crm-data-security/

7 - Most Common CRM Security Concerns and Solutions. [Електронний ресурс] – Режим доступу: https://www.wheelhouse.com/resources/most-common-crm-security-concerns-and-solutions-a9953

8 – From cyber attacks to Insider Threars. [Електронний ресурс] – Режим доступу: https://www.talisma.com/from-cyber-attacks-to-insider-threats-how-crm-security-can-safeguard-your-data/

9 - Threat Landscape in CRM Security. [Електронний ресурс] – Режим доступу: https://www.qique.cn/open_back/learn/article?cateTypeId=0&id=23786

10 - GLOBAL CRM PROVIDER EXPOSED MILLIONS OF CLIENTS' FILES ONLINE. [Електронний ресурс] – Режим доступу: https://securityaffairs.com/151999/data-breach/crm-provider-really-simple-systems-data-leak.html

11 - Загальний регламент про захист даних (GDPR). [Електронний ресурс] – Режим доступу: https://gdpr-text.com/uk/

12 - Top 10 ways to protect organisations from cyber attacks. [Електронний ресурс] – Режим доступу: https://technologymagazine.com/top10/top-10-ways-to-protect-organisations-from-cyber-attacks

13 - How Can I Protect My Company From Cyber-Attacks? [Електронний ресурс] – Режим доступу: https://cypfer.com/resource/how-can-i-protect-my-company-from-cyber-attacks/

14 - Use of cognitive mapping techniques in information systems development. [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/286992310_Use_of_cognitive_mapping_techniques_in_information_systems_development

15 - How to build a cognitive map. https://www.nature.com/articles/s41593-022-01153-y

16 - Threat modeling vs vulnerability assessment. [Електронний ресурс] – Режим доступу: https://www.practical-devsecops.com/threat-modeling-vs-risk-assessment/

17 - Comparing DREAD, STRIDE, and PASTA Threat Models. [Електронний ресурс] – Режим доступу: https://bluegoatcyber.com/blog/comparing-dread-stride-and-pasta-threat-models-which-is-most-effective/

18 - Threat Modeling: 12 Available Methods. [Електронний ресурс] – Режим доступу: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

19 - What is CRM and How Does it Work? . [Електронний ресурс] – Режим доступу: https://www.creatio.com/crm/what-is-crm

20 - Cyber Threats and Advisories. [Електронний ресурс] – Режим доступу: https://www.cisa.gov/topics/cyber-threats-and-advisories

21 - Types of Cyberthreats. [Електронний ресурс] – Режим доступу: https://www.ibm.com/think/topics/cyberthreats-types

ДОДАТОК

```
import tkinter as tk
from tkinter import messagebox

class CyberSecurityApp:
    def __init__(self, root):
        self.root = root
        self.root.title("Визначення зрілості компанії")

        self.score = 0
        self.questions = [
            "IDS/IPS", "Шифрування даних", "MFA", "Антивірусне ПЗ",
            "Політики управління доступом", "Процедури управління інцидентами",
"Політика резервного копіювання",
            "Застосування GDPR/NIST", "Методичні матеріали по кібергігієні",
            "Проведення тестування на знання дій у випадках реалізації загрози",
            "Проведення тренінгів по кібербезпеці",
            "Періодичне оновлення даних для авторизації"
        ]
        self.answers = {}

        self.create_main_interface()

    def create_main_interface(self):
        self.start_button = tk.Button(self.root, text="Пройти оцінювання",
command=self.start_assessment)
        self.start_button.pack(pady=20)

    def start_assessment(self):
```

```
        self.assessment_window = tk.Toplevel(self.root)
        self.assessment_window.title("Визначення зрілості компанії")

        for i, question in enumerate(self.questions):
            tk.Label(self.assessment_window, text=question).grid(row=i, column=0, padx=10, pady=5)
            self.answers[question] = tk.StringVar(value="ні")
            tk.Radiobutton(self.assessment_window, text="Так", variable=self.answers[question], value="так").grid(row=i, column=1)
            tk.Radiobutton(self.assessment_window, text="Ні", variable=self.answers[question], value="ні").grid(row=i, column=2)

        self.calculate_button = tk.Button(self.assessment_window, text="Обрахувати захищеність", command=self.calculate_score)
        self.calculate_button.grid(row=len(self.questions), column=0, columnspan=3, pady=10)

    def calculate_score(self):
        self.score = sum(1 for answer in self.answers.values() if answer.get() == "так")

        self.assessment_window.destroy()

        if self.score <= 4:
            level = "слабкий рівень захищенності"
        elif 5 <= self.score <= 7:
            level = "середній рівень захищенності"
        elif 8 <= self.score <= 10:
            level = "достатній рівень захищенності"
        else:
            level = "високий рівень захищенності"
```

```
        messagebox.showinfo("Результат оцінювання", f"Ви набрали {self.score} балів: {level}")


if __name__ == "__main__":
    root = tk.Tk()
    app = CyberSecurityApp(root)
    root.mainloop()
```