Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Розробка пропозицій щодо підвищення рівня захисту персональних даних у контексті кібервійни
(тема)

Виконала:
студентка 2 курсу, групи АМСЗІм-21-2
Товкун Ю.І.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Добринін І.С.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Товкун Юлії Ігорівні
(прізвище, ім'я, по батькові)

1. Тема роботи: Розробка пропозицій щодо підвищення рівня захисту персональних даних у контексті кібервійни
затверджена наказом по університету від «23» березня 2023р. №292 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 15.05.2023р.
3. Вихідні дані до роботи: законодавство України у сфері захисту персональних даних, GDPR, дані про кібератаку, модель загроз STRIDE, модель оцінювання ризиків CVSS v3.1.
4. Перелік питань, що потрібно опрацювати в роботі:
1) Виявлення законодавчих вимог для пом'якшення загроз безпеки та конфіденційності.
2) Кіберінциденти в контексті кібервійни, які спрямовані на персональні дані.
3) Застосування моделювання загроз для зниження ризиків безпеки під час обробки персональних даних.
4) Оцінка ефективності проаналізованих методів пом'якшення загроз недоторканності приватного життя з точки зору ризиків безпеки та конфіденційності, використовуючи модель оцінки ризиків.

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: демонстраційний матеріал у вигляді ppt-презентації.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Добринін Ігор Станіславович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	15.02.2023	Виконано
2	Збір матеріалів для дослідження	01.03.2023	Виконано
3	Розробка 1 розділу	20.03.2023	Виконано
4	Розробка 2 розділу	07.04.2023	Виконано
5	Розробка 3 розділу	15.04.2023	Виконано
6	Розробка 4 розділу	22.04.2023	Виконано
7	Оформлення кваліфікаційної роботи	30.04.2023	Виконано

Дата видачі завдання 15 лютого 2023 року

Студентка _____ Товкун Ю.І.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Добринін І.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с., 17 рис., 9 таблиць, 2 додатка, 25 джерел.

ІНФОРМАЦІЙНА БЕЗПЕКА, ПЕРСОНАЛЬНІ ДАНІ, МОДЕЛЮВАННЯ ЗАГРОЗ, ОЦІНКА РИЗИКІВ.

Об’єкт дослідження – процес захисту персональних.

Предмет дослідження – методи та технології підвищення рівня захисту персональних даних у військових конфліктах, зокрема російсько-української війни.

Мета роботи – розробка пропозицій щодо підвищення рівня захисту персональних даних у контексті кібервійни та виявлення шляхів вирішення проблеми захисту персональних даних.

Методи досліджень – аналіз наявних теоретичних джерел, синтез інформації, експертний аналіз, моделювання загроз, аналіз кібератак, аналіз методів захисту персональних даних, оцінка ризиків.

Сучасний світ все більше стає цифровим, а кіберпростір стає полем військових конфліктів, зокрема російсько-української війни. У зв'язку з цим, проблема захисту персональних даних набуває особливого значення, оскільки порушення їх конфіденційності може призвести до порушення прав людини та національної безпеки.

Дана робота містить опис основних вимог GDPR та українських законів у сфері захисту персональних даних. Також міститься аналіз кібератаки, яка спричинила виток персональних даних. У ході роботи було розроблено модель загроз відповідно до додатку, у якому було спричинено виток персональних даних. Було запропоновано рекомендації по поліпшенню, які могли б запобігти подальшим витокам даних. Було зроблено оцінку ризиків відповідно до розробленої моделі загроз.

ABSTRACT

The report contains: 76 p., 17 fig., 9 tables, 2 application, 25 sources.

INFORMATION SECURITY, PERSONAL DATA, THREAT MODELING, RISK ASSESSMENT.

The object of research is the process of personal data protection.

The subject of the study is methods and technologies for improving the level of personal data protection in military conflicts, in particular the Russian-Ukrainian war.

Purpose - to develop proposals for improving the level of personal data protection in the context of cyber warfare and to identify ways to solve the problem of personal data protection.

Research methods: analysis of available theoretical sources, synthesis of information, expert analysis, threat modeling, analysis of cyberattacks, analysis of personal data protection methods, risk assessment.

The modern world is increasingly becoming digital, and cyberspace is becoming a field of military conflicts, including the russian-ukrainian war. In this regard, the issue of personal data protection is of particular importance, as a breach of its confidentiality may lead to violations of human rights and national security.

This paper describes the main requirements of the GDPR and Ukrainian laws in the field of personal data protection. It also analyzes the cyberattack that led to the personal data leak. In the course of the work, a threat model was developed in accordance with the application in which the personal data leakage occurred. Recommendations for improvements that could prevent further data leaks were proposed. A risk assessment was made in accordance with the developed threat model.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЄС – Європейський Союз

ІПН – ідентифікаційний податковий номер

ПІБ – прізвище, ім'я, по батькові

ФОП – фізична особа підприємець

API – application programming interface

BPMN – business process model and notation

CERT-UA – computer emergency response team of Ukraine

CIS – center for internet security

CMS – content management system

CVSS – common vulnerability scoring system denial of service

DFD – data flow diagrams

DPO – data protection officer

FIRST – forum of incident response and security teams

GDPR – general data protection regulation

HTTPS –hypertext transfer protocol secure

ID – identity document

JNDI – java naming and directory interface

ISO – international organization for standardization

JSON – java script object notation

JWT – JSON web token

MBR – master boot record

Microsoft SDL –security development lifecycle

NIST SP – national institute of standards and technology special publication

OCTAVE – operationally critical threat, asset, and vulnerability evaluation

OWASP SAMM – open web application security project security assurance maturity model

PASTA – process for attack simulation and threat analysis

RTO – recovery time objective

RSA – rivest-shamir-adleman

SBOM – software bill of materials

SQL – structured query language

SSL/TLS – secure sockets layer / transport layer security

STRIDE – spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege

TRIKE – team readiness and incident kernel evaluation

URL – uniform resource locator

VAST – visual, agile, and simple threat modeling

XSS – cross-site scripting

ВСТУП

Сучасний світ стає все більш цифровим, а кіберпростір набуває значущості у військових конфліктах. Однією з ключових проблем, пов'язаних з кібервійнами, є захист персональних даних користувачів. Викрадення та зловживання персональними даними можуть мати серйозні наслідки як для окремих осіб, так і для національної безпеки держави.

Актуальність теми безперечна у зв'язку з тим, що атаки на інформаційні системи та персональні дані можуть мати катастрофічні наслідки для економіки, національної безпеки та приватності громадян. Зростання кількості кібератак, що мають на меті викрадення персональних даних, підкреслює важливість розробки ефективних механізмів їх захисту [1]. Також є необхідність розробки нових та вдосконалення існуючих підходів до захисту персональних даних у кіберпросторі, особливо в умовах військових конфліктів. Це допоможе забезпечити стабільність та безпеку інформаційних систем, зменшити ризики втрати конфіденційності та приватності, а також підвищити ефективність боротьби з кіберзлочинністю.

Актуальність теми також посилюється через поширення нових технологій, таких як Інтернет речей (IoT), хмарні обчислення, штучний інтелект та машинне навчання, які створюють нові можливості для кіберзлочинців та збільшують складність забезпечення захисту персональних даних. Окрім того, пандемія COVID-19 спричинила стрімке збільшення віддаленої роботи та онлайн-взаємодії, що стало додатковим чинником, який підвищує ризики кібератак і порушень захисту персональних даних [1].

У світлі глобалізації та розвитку міжнародної співпраці в галузі кібербезпеки, актуальність теми полягає також у необхідності врахування міжнародних стандартів та досвіду різних країн у розробці пропозицій щодо підвищення рівня захисту персональних даних. Важливо розглянути можливості підвищення рівня кібербезпеки на національному рівні через посилення законодавчих, технічних та організаційних заходів [1].

Отже, розробка пропозицій щодо підвищення рівня захисту персональних даних у контексті кібервійни є дуже актуальною темою для сучасного суспільства. Вивчення

цього питання сприятиме забезпеченню цілісності, доступності та конфіденційності інформації, зміцненню національної безпеки та забезпеченню ефективного відповідного реагування на загрози кіберпростору.

Метою роботи є розробка пропозицій щодо підвищення рівня захисту персональних даних у контексті кібервійни та виявлення шляхів вирішення проблеми захисту персональних даних.

Для вирішення поставленої задачі, в першому розділі кваліфікаційної роботи проведено аналіз захисту персональних даних відповідно до GDPR та закону України «Про захист персональних даних». У другому розділі роботи було проведено аналіз кібератаки, яка спричинила виток даних з додатку, який відображував персональні дані користувачів. У зв’язку з цим, у третьому розділі було розроблено модель загроз для додатку на базі існуючої моделі STRIDE, та запропоновано рекомендації по протидії знайденим загрозам. У четвертому розділі було проведено оцінку ризиків за допомогою моделі CVSS v3.1 та порівняно результати до впровадження рекомендацій по протидії знайденим загрозам та після.

1 ЗАКОНОДАВЧІ ВИМОГИ ДЛЯ ПОМ'ЯКШЕННЯ ЗАГРОЗ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ

Тема захисту персональних даних є актуальною в сучасному світі, що пов'язано зі зростаючим використанням цих даних в різних організаціях. Неможливо уявити фінансові установи, які не зберігають та не обробляють інформацію про співробітників, клієнтів тощо.

Отже, витік персональних даних може завдати величезної шкоди бізнесу. Крім того, захист персональних даних є вимогою законодавства, і ці вимоги будуть тільки посилюватися з ростом використання цифрового документообігу.

1.1 Захист персональних даних відповідно до українського законодавства

В Україні захист персональних даних регулюється Конституцією, яка в частині 2 статті 32 передбачає, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [2]. Також захист персональних даних регулюється Законом України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI [3] та Законом України «Про інформацію» від 02.10.1992 р. № 2657-XII [4].

Законодавство не містить чіткого переліку того, що відноситься до персональних даних. Це будь-яка інформація, яка ідентифікує фізичну особу або може її ідентифікувати, але це поняття досить широке. Наприклад, відповідно до статті 11 Закону України «Про інформацію» до конфіденційної інформації про фізичну особу належать відомості про її національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, а також адреса, дата і місце народження [4].

Перелік персональних даних конкретизувався після прийняття Конституційним Судом України Рішення № 2-2012 від 20 січня 2012 року, в якому зазначено, що інформацією про особисте та сімейне життя, тобто персональними даними про особу, є будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [5], зокрема, такі як:

– національність;
– освіта;
– сімейний стан;
– релігійні переконання;
– стан здоров'я;
– матеріальне становище;
– адреса;
– дата та місце народження;
– місце проживання, перебування;
– дані про особисті майнові та немайнові відносини цієї особи з іншими фізичними особами, у тому числі членами сім'ї;
– відомості про події та явища, що відбулися або відбуваються у побутовій, інтимній, дружній, професійній, діловій та інших сферах життя особи.

Така інформація про фізичну особу є конфіденційною і може бути поширена лише за її згодою, крім випадків, визначених законом, і лише в інтересах захисту прав людини.

Існують також персональні дані, які становлять особливий ризик для прав і свобод суб'єктів. Відповідно до Наказу Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 р. № 1-14 [6] – це дані:

– расового, етнічного та національного походження;
– політичні, релігійні або світоглядні переконання;
– членство в політичних партіях або організаціях;
– стан здоров'я;
– статевого життя;
– біометричні дані;
– генетичні дані;
– притягнення до адміністративної чи кримінальної відповідальності;
– застосування до особи заходів у рамках досудового розслідування.

Збір та обробка таких персональних даних здійснюється за спеціальними правилами. Ті, хто збирає чи іншим чином обробляє такі персональні дані про

фізичних осіб, зобов'язані повідомляти Омбудсмана про їх збирання, обробку, зміну, припинення обробки протягом 30 днів, а також мати структурний підрозділ, відповідальний за обробку, та повідомити про створення такого підрозділу в установленому порядку. Порядок виконання всіх цих обов'язків міститься в тому ж таки дорученні Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1-14. Інформація про таких осіб публікується на офіційному веб-сайті Омбудсмана.

1.2 Захист персональних даних відповідно до GDPR

Наразі Україна розглядає можливість удосконалення законодавства про захист персональних даних з метою приведення його у відповідність до європейських стандартів, а саме GDPR, оскільки Україна прагне стати членом ЄС, а відповідність GDPR є важливим кроком для приведення законодавства про захист персональних даних у відповідність до правової бази ЄС. Отже, нижче наведені основні моменти захисту персональних даних відповідно до GDPR [7].

GDPR спрямований на імплементацію законів про захист персональних даних у країнах-членах ЄС, захист прав на недоторканність приватного життя резидентів ЄС та розширення прав і можливостей людей шляхом надання їм більшого контролю над своїми персональними даними. З регламенту можна виокремити такі основні риси [8].

1) Щодо сфери застосування, то GDPR поширюється на всі організації, які обробляють персональні дані резидентів ЄС, незалежно від місцезнаходження організації.

2) Також регламент містить чітке визначення персональних даних, а саме зазначає, що персональні дані – це будь-яка інформація, що стосується фізичної особи, яка ідентифікована або може бути ідентифікована (суб'єкт даних).

3) Щодо прав суб'єкта даних, то згідно з GDPR, суб'єкти даних мають право на доступ, виправлення, видалення, обмеження обробки, заперечення проти обробки та перенесення даних. Так само організації повинні отримати чітку, поінформовану та однозначну згоду суб'єктів даних перед тим, як обробляти їхні дані.

4) Що стосується мінімізації даних, організації повинні збирати та обробляти лише ті персональні дані, які необхідні для конкретної, законної мети.

5) Організації повинні впроваджувати захист персональних даних на етапі проектування та забезпечувати, щоб захист даних був налаштуванням за замовчуванням.

6) Крім того, у разі витоку даних організації повинні повідомити відповідний наглядовий орган протягом 72 годин, а також поінформувати постраждалих суб'єктів даних без невиправданої затримки.

7) Важливим моментом є також відповідальний за захист даних (DPO). Організації повинні призначити відповідального за дотримання GDPR.

8) Передача даних до країн, що не є членами ЄС, повинна відповідати вимогам GDPR, таким як рішення про адекватність, стандартні договірні положення або обов'язкові корпоративні правила.

9) Нарешті, штрафи та покарання, а саме: організації, визнані порушниками GDPR, можуть бути піддані значним штрафам у розмірі до 20 мільйонів євро або 4% від їхнього річного глобального обороту, залежно від того, яка з цих сум є більшою.

1.3 Порівняння та визначення недоліків щодо захисту персональних даних в українському законодавстві порівняно з вимогами GDPR

Загалом, на основі Закону України «Про захист персональних даних» та аналізу положень GDPR можна виділити декілька вимог до збору, зберігання, обробки та використання персональних даних [3]. Опис вимог можна побачити в таблиці А.1 у додатку А.

Виходячи з вимог українського законодавства, які зазначені в таблиці А.1 у додатку А, можна зробити висновок, що вони в першу чергу спрямовані на забезпечення збору та обробки персональних даних у справедливий та законний спосіб та на захист прав на приватність суб'єктів даних, але в той же час існують очевидні прогалини в законодавстві, виходячи, наприклад, з порівняння з GDPR [8]:

1) Відсутність інформації про оцінку ризиків – в українському законодавстві немає згадки про комплексну оцінку ризиків, яка є важливим елементом захисту персональних даних, тоді як у GDPR зазначено, що контролери повинні враховувати сучасний стан, витрати на впровадження, характер та обсяг обробки, а також ризики для прав і свобод суб'єктів даних при виборі відповідних заходів безпеки.

2) Відсутність псевдонімізації та шифрування інформації – GDPR згадує псевдонімізацію та шифрування як потенційні заходи безпеки на основі оцінки ризиків. У свою чергу, ці методи прямо не згадуються в українському законодавстві.

3) Відсутність регулярного тестування та оцінки безпеки – в українському законодавстві не згадується вимога щодо регулярного тестування, оцінки та аналізу ефективності технічних та організаційних заходів.

4) Відсутність повідомлення суб'єктів даних про порушення даних – в українському законодавстві відсутня вимога повідомляти суб'єктів даних про порушення персональних даних, якщо це може призвести до високого ризику для їхніх прав і свобод.

5) Відсутність прав, пов'язаних з автоматизованим прийняттям рішень та профілюванням – українське законодавство не згадує про надання суб'єктам права не бути об'єктом рішення, що ґрунтується виключно на автоматизованій обробці, включаючи профілювання, яке призводить до правових наслідків або подібних істотних наслідків. У свою чергу, GDPR згадує про це право, і це право допомагає захистити суб'єктів даних від потенційної шкоди, спричиненої автоматизованими кібератаками або неправомірним використанням їхніх даних.

6) Нечіткість положень – українському законодавству бракує чіткості в положеннях, що може призвести до плутанини та невизначеності щодо вимог до контролерів даних та прав суб'єктів даних.

7) Відсутність положень про транскордонну передачу даних в межах Європейського Союзу – закон передбачає обмеження на передачу персональних даних за межі України, але не розглядає передачу персональних даних між Україною та іншими країнами Європейського Союзу.

Лише усунувши ці прогалини в українському законодавстві, Україна зможе зміцнити свою правову базу та краще захистити персональні дані своїх громадян від кібератак.

2 КІБЕРІНЦИДЕНТИ В КОНТЕКСТІ КІБЕРВІЙНИ, ЯКІ СПРЯМОВАНІ НА ПЕРСОНАЛЬНІ ДАНІ

Розглядаючи випадок України в стані кібервійни більш детально, можна зробити висновок, що персональні дані наразі є надто вразливими, оскільки урядові та військові організації обробляють великі обсяги даних як про цивільне населення, так і про військовослужбовців, витоки яких можуть створити проблеми безпосередньо для наземних військових операцій, таких як фільтраційні заходи, оскільки вони передбачають збір персональних даних у великих обсягах та подальшу обробку цих даних [9].

Це становить значний ризик як для недоторканності приватного життя, так і для індивідуальних даних. Фільтрація також відбувається в контексті військової та розвідувальної діяльності, де зберігається ризик крадіжки даних осіб, які не беруть безпосередньої участі в конфлікті, але можуть ненавмисно стати мішенню або їхні персональні дані можуть бути зібрані та проаналізовані [10].

2.1 Аналіз кібератаки на платформу «Дія»

Однією з найбільших кібератак на персональні дані напередодні початку російсько-української війни є атака на портал «Дія». «Дія» – це створена українським урядом цифрова платформа, яка надає громадянам доступ до низки державних послуг, зокрема можливість зберігати та керувати документами, що посвідчують особу [11].

Додаток «Дія» дозволяє користувачам зберігати свій електронний паспорт, водійське посвідчення та інші документи, що посвідчують особу. Він також надає доступ до кількох державних послуг, зокрема подання податкових декларацій, отримання соціальних виплат та реєстрації бізнесу. Інтерфейс порталу можна побачити на рисунку 2.1.

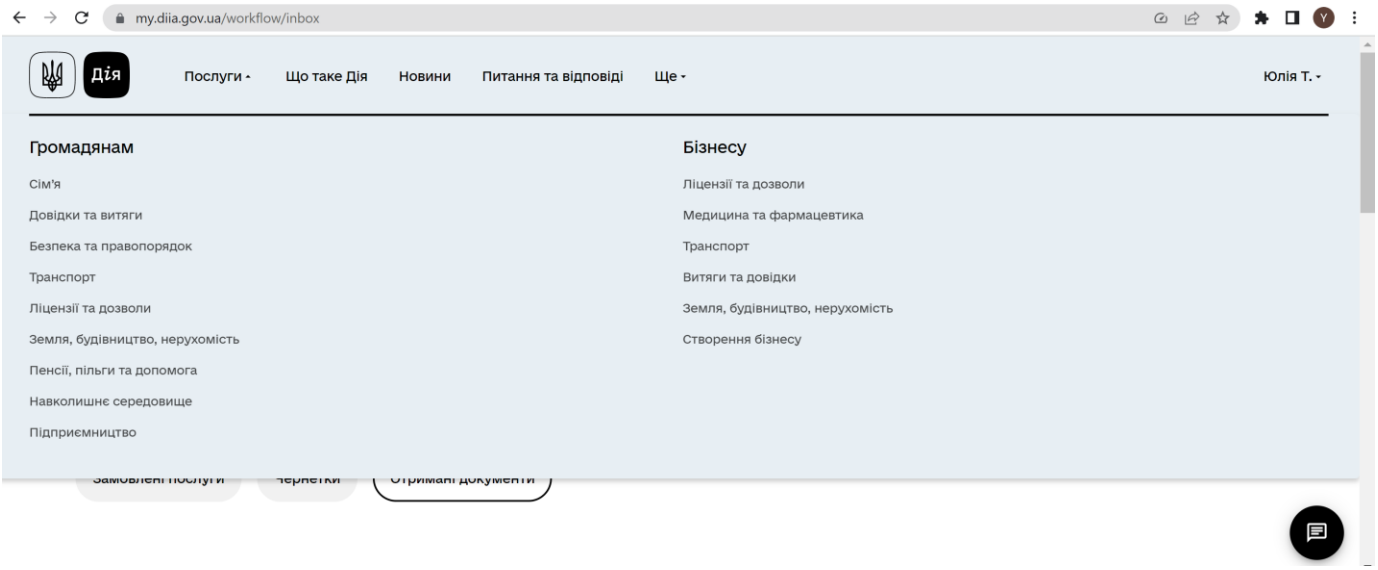


Рисунок 2.1 – Інтерфейс порталу «Дія»

На початку січня 2022 року з'явилася інформація про продаж даних двох мільйонів українців, які зберігалися на порталі «Дія». Дані були виставлені на продаж на різних форумах, а трохи пізніше до вже вкрадених даних додалися дані з реєстру е-водіїв. Реєстр – це особистий електронний кабінет водія, де користувач може знайти інформацію про транспортний засіб, отримати різні довідки, пов'язані з транспортним засобом тощо [12].

Після атаки кіберполіція заперечила, що портал був зламаний, і заявила, що витік даних не може бути пов'язаний з цією кібератакою, оскільки «Дія» не зберігає дані на сервері, а використовує підхід data-in-transition [13]. Інформація про це також міститься в політиці конфіденційності додатку, фрагмент якої наведено на рисунку 2.2.

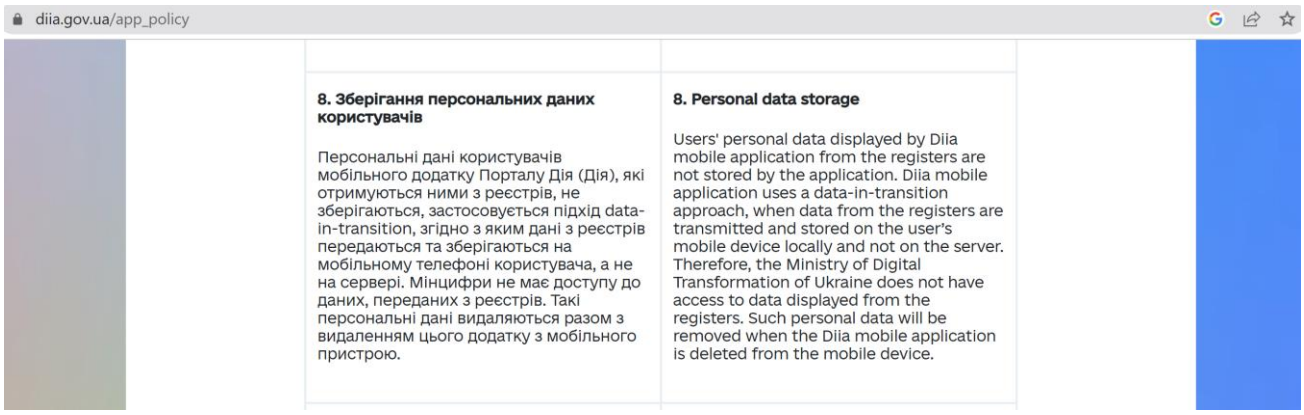


Рисунок 2.2 – Політика конфіденційності «Дії» щодо зберігання персональних даних

Хоча офіційного підтвердження витоку даних не було, але на хакерському форумі RaidForums база даних була виставлена на продаж за ціною понад $80 000 [13]. Частину витоку бази даних можна побачити на рисунку 2.3 [12].

```
BACKEND_FORCE_SECURE=true
LINK_POLICY=secure

APP_ENV=prod

APP_URL=http://diia.gov.ua
APP_THEME=diia

DB_HOST=192.168.3.48

DB_DATABASE=prod-diia
DB_USERNAME=prod-diia
DB_PASSWORD=d5Re9rJ53C73ve5HAAQa3f29J

QUEUE_DRIVER=database

REDIS_HOST=192.168.3.44
REDIS_PASSWORD=VYA92bwmLE9APJfb
REDIS_PORT=6379
CACHE_DRIVER=redis
SESSION_DRIVER=redis

MAIL_DRIVER=smtp
MAIL_HOST=192.168.100.5
MAIL_PORT=25
MAIL_ENCRYPTION=null
MAIL_USERNAME=null
MAIL_PASSWORD=null
```

Рисунок 2.3 – Частина витоку бази даних

Що стосується архівів даних, які стали доступними, то вони поділяються на кілька типів.

У першому архіві зберігалася база персональних даних, а саме: електронна пошта, номер телефону, ПІБ, ІПН, адреса, серія, номер, дата видачі паспорта, назва

органу, що його видав, номер і дата видачі ID-картки. Крім того, база даних містила унікальний ідентифікатор, що складається з цифр і букв [14].

Другий архів містив фотографії документів, а саме: внутрішнього паспорта, студентського квитка, закордонного паспорта тощо.

Третій архів складався з бази даних записів з різними даними, інформацією про звернення за допомогою, квитанціями про оплату тощо. Кожен запис також мав унікальний ідентифікатор.

Коли користувач заходить на портал «Дія», додаток вставляє JWT-токен, в якому зашифровані такі дані, як ім'я, прізвище та унікальний ідентифікатор. Цей ідентифікатор збігається з ідентифікаторами, знайденими в архівах, перерахованих вище [12]. За допомогою коду, наведеного нижче, можна знайти унікальний ідентифікатор, згенерований порталом:

```
JSON.parse(atob(localStorage.getItem('token').split('.')[1])).userId.
```

Формат JWT-токену (жовта лінія) та унікального ідентифікатора (зелена лінія) можна побачити на рисунку 2.4.

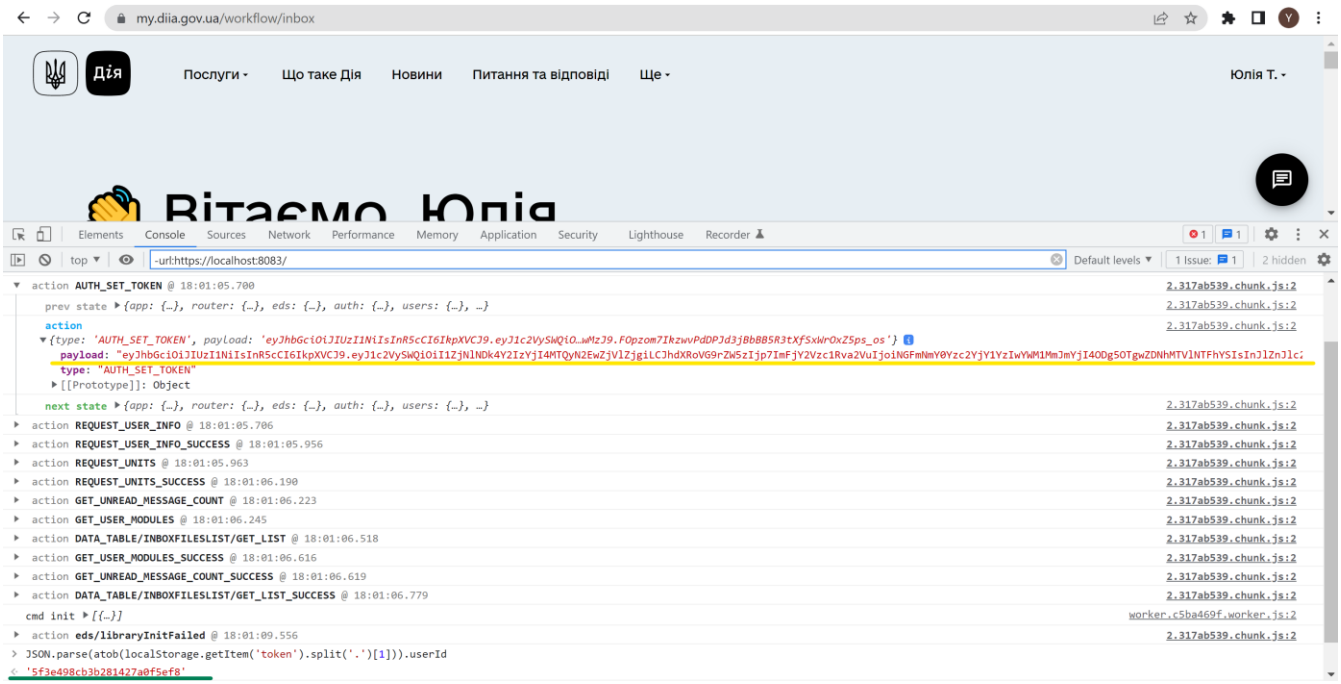


Рисунок 2.4 – JWT токен та унікальний ідентифікатор

Це можна перевірити, звіривши свій ідентифікатор, який генерується порталом, з ідентифікаторами, знайденими у зламаній базі даних. За 2 тижні перевірок звичайними користувачами було знайдено 54 збіги з 1500 перевірок, що вже суперечить офіційній заяві про те, що витоку даних не було [14].

Точного пояснення, як саме стався витік даних, немає, адже за офіційною інформацією, система відображення даних на порталі «Дія» налаштована таким чином, що при кожному запиті документи підтягуються з реєстрів, які зберігаються на віддалених серверах і не пов'язані між собою, а отже, немає окремої бази даних, де б зберігалися всі документи [16].

2.2 Аналіз вразливостей, через які була спрямована атака

Було розглянуто декілька варіантів кібератак на портал «Дія», зокрема, використання вразливостей log4j та OctoberCMS.

Log4j – це широко використовувана бібліотека логування з відкритим вихідним кодом для Java-додатків, що підтримується Apache Software Foundation. Наприкінці грудня 2021 року було виявлено критичну уразливість у бібліотеці Log4j для версій 2.0-2.14.1 – Log4Shell. Уразливість була спричинена функціоналом Java Naming and Directory Interface бібліотеки, який дозволяв віддалене виконання коду через використання спеціально сконструйованих рядків [10].

Зловмисники можуть скористатися цією уразливістю, відправивши шкідливий рядок, наприклад, «${jndi:ldap://[malicious_server]}» до вразливого додатку.

Log4j спробує активувати цей рядок через JNDI, що призведе до того, що Java-додаток підключиться до сервера зловмисника і, можливо, виконає випадковий код [11].

Ця уразливість може вплинути на багато додатків, включаючи «Diia», і може спровокувати такі вектори атаки, як:

– надсилання шкідливого вводу до веб-додатків, серверів або інших сервісів, які використовують Log4j для ведення журналів;

– ведення шкідливих рядків в агенти користувачів, реферали або інші HTTP-заголовки, які реєструються додатком.

Що стосується вразливостей в OctoberCMS, то це система управління контентом з відкритим вихідним кодом, що базується на PHP-фреймворку Laravel. Розглянемо одну з уразливостей, яка ймовірно мала місце під час атаки на портал «Дія», а саме CVE-2020-26229. Це Cross-Site Scripting (XSS) уразливість в OctoberCMS версії 1.0.470 та вище. Дана уразливість дозволяє зловмиснику впровадити шкідливий JavaScript-код в CMS за допомогою спеціально створеного корисного навантаження, щоб отримати несанкціонований доступ до конфіденційних даних, виконати довільний JavaScript-код в контексті браузера користувача або виконати дії від імені жертви. Хоча оновлення програмного забезпечення, яке закриває цю вразливість, було випущено майже одразу після її виявлення, IT-спеціалісти українських відомств могли не встигнути вчасно оновити програмне забезпечення до версії без цієї вразливості [13].

Вектори атаки для використання цієї вразливості включають:

– створення шкідливих даних для форм або інших полів у CMS для зберігання XSS-шкідливого коду;

– обман користувачів для переходу за шкідливими посиланнями або взаємодії зі шкідливим контентом, який впроваджує шкідливе навантаження в CMS [14].

Згідно з аналізом CERT-UA – Українська урядова команда реагування на комп'ютерні надзвичайні ситуації, яка діє при Державній службі спеціального зв'язку та захисту інформації України, також припустила, що зловмисники могли здійснити атаку через вразливості в жовтневій CMS, але все ж таки погодилася з тим, що кібератака, яка сталася в січні 2022 року, була здійснена з використанням шкідливого програмного забезпечення WhisperGate [15].

WhisperGate – це шкідлива програма, призначена для пошкодження файлів. Кібератака була спрямована на різні українські урядові веб-сайти, включаючи портал «Дія», і складалася з двох етапів [15]. На першому етапі шкідлива програма перезаписувала головний завантажувальний запис (MBR) фальшивим повідомленням з вимогою викупу, що перешкоджало завантаженню системи. На другому етапі атаки через троянський завантажувач завантажувалося шкідливе програмне забезпечення, яке пошкоджувало файли, перезаписуючи їх вміст на певну кількість байт.

Атака відбувається поетапно, на першому етапі шкідливе ПЗ під назвою stage1.exe впроваджується в різні каталоги системи жертви, такі як C:\ProgramData, C: та C:\temp. Шкідливе програмне забезпечення виконується за допомогою інструменту Impacket, який дозволяє зловмисникам переміщатися в мережі жертви, цей інструмент є загальнодоступним [16].

Після запуску двоетапне шкідливе програмне забезпечення перезаписує головний завантажувальний запис (MBR) в системі жертви запискою з вимогою викупу. MBR відповідає за інструкції для завантаження операційної системи комп'ютера. Вимога містить адресу біткоїн-гаманця та унікальний ідентифікатор облікового запису (Tox ID), який використовується в протоколі зашифрованих повідомлень Tox [15].

Шкідливе програмне забезпечення запускається, коли жертва вимикає свій пристрій, що є незвичним для цього типу атак.

Крім того, вимога викупу не має сенсу і є відволікаючим маневром, оскільки шкідливе програмне забезпечення знищує MBR і всі файли, на які воно націлене.

Зазвичай атаки з вимогою викупу розробляються індивідуально для кожної жертви, але в цьому випадку було використано одне й те саме корисне навантаження для кількох жертв. Крім того, в той час як більшість програм-здирників шифрують файли, ця шкідлива програма знищує їх, перезаписуючи MBR, що унеможливлює відновлення [15].

Крім того, злочинці не вказують у вимогах суми платежу або адреси криптовалютних гаманців, але у вимозі WhisperGate ця інформація містилася. У всіх випадках WhisperGate була вказана одна і та ж адреса біткоїн-гаманця [16].

Крім того, дуже незвично, що спілкування з жертвами відбувається виключно через Tox ID. Зазвичай зловмисники надають кілька способів зв'язку, наприклад, форуми підтримки або електронну пошту, щоб полегшити успішний контакт з жертвою.

Нарешті, більшість записок про викуп містять ідентифікатор користувача, який жертва повинна надіслати зловмисникам, щоб отримати ключ розшифровки. Однак у цьому випадку повідомлення про викуп не містить ідентифікатора користувача.

На другому етапі атаки знищувач шкідливих файлів завантажується за допомогою програми під назвою Stage2.exe. Після виконання Stage2.exe завантажує

руйнівник із каналу Discord із жорстко закодованим у програмі посиланням для завантаження [15]. Шкідлива програма шукає файли певних типів, які зображені на рисунку 2.5, у певних каталогах системи [12].

```
.HTML .HTM .SHTML .XHTML .PHTML .PHP .JSP .ASP .PHPS .PHP5 .ASPX .PHP4 .PHP6
.PHP7 .PHP3 .DOC .DOCX .XLS .XLSX .PPT .PPTX .PST .OST .MSG .EML .VSD .VSDX
.TXT .CSV .RTF .WKS .WK1 .PDF .DWG .ONETOC2 .SNT .JPEG .JPG .DOCB .DOCM
.DOT .DOTM .DOTX .XLSM .XLSB .XLW .XLT .XLM .XLC .XLTX .XLTM .PPTM .POT
.PPS .PPSM .PPSX .PPAM .POTX .POTM .EDB .HWP .602 .SXI .STI .SLDX .SLDM
.BMP .PNG .GIF .RAW .CGM .SLN .TIF .TIFF .NEF .PSD .AI .SVG .DJVU.SH .CLASS
.JAR .BRD .SCH .DCH .DIP .PL .VB .VBS .PS1 .BAT .CMD .JS .ASM .H .PAS .CPP
.C .CS .SUO .ASC .LAY6 .LAY .MML .SXM .OTG .ODG .UOP .STD .SXD .OTP .ODP
.WB2 .SLK .DIF .STC .SXC .OTS .ODS .3DM .MAX .3DS .UOT .STW .SXW .OTT .ODT
.PEM .P12 .CSR .CRT .KEY .PFX .DER .OGG .RB .GO .JAVA .INC .WAR .PY .KDBX
.INI .YML .PPK .LOG .VDI .VMDK .VHD .HDD .NVRAM .VMSD .VMSN .VMSS .VMTM
.VMX .VMXF .VSWP .VMTX .VMEM .MDF .IBD .MYI .MYD .FRM .SAV .ODB .DBF .DB
.MDB .ACCDB .SQL .SQLITEDB .SQLITE3 .LDF .SQ3 .ARC .PAQ .BZ2 .TBK .BAK .TAR
.TGZ .GZ .7Z .RAR .ZIP .BACKUP .ISO .VCD .BZ .CONFIG
```

Рисунок 2.5 – Список розширень файлів, які перезаписуються

Коли програма знаходить файл із одним із цих розширень, вона замінює вміст файлу фіксованою кількістю байтів 0xCC, пошкоджуючи файл і роблячи його марним. Зрештою, зловмисне програмне забезпечення змінює назву пошкодженого файлу на чотирибайтне розширення, яке здається випадковим [15].

Описаний вище кіберінцидент на порталі «Дія» за результатом можна прирівняти до крадіжки документів, оскільки в Україні документи з електронного порталу мають таку ж юридичну силу, як і фізичні документи.

2.3 Формування рекомендацій щодо зберігання персональних даних та аналіз недоліків, відповідно до кібератаки

На основі аналізу кібератаки WhisperGate можна виділити кілька вимог і рекомендацій щодо зберігання персональних даних, щоб уникнути подібних витоків у майбутньому. Короткий перелік вимог можна побачити в таблиці 2.1.

Таблиця 2.1 – Рекомендації до програми, яка зберігає персональні дані на основі впливу проаналізованої кібератаки WhisperGate та вразливості log4j, OctoberCMS

Назва вимоги	**Елементи вимоги**
1	2
Безпечна мережева інфраструктура	– брандмауер – може допомогти запобігти несанкціонованому доступу до мережі, блокуючи зловмисний трафік і фільтруючи небажаний трафік; – система виявлення та запобігання вторгненням (IDPS) – може виявляти та запобігати спробам вторгнення в режимі реального часу, а також може сповіщати персонал служби безпеки про вжиття відповідних заходів; – віртуальна приватна мережа (VPN) – може допомогти запобігти несанкціонованому доступу до мережі та може обмежити потенційну шкоду, спричинену кібератакою; – шифрування даних – може допомогти захистити конфіденційні дані від перехоплення та читання хакерами; – сегментація мережі – процес поділу мережі на менші сегменти для запобігання поширенню кібератаки. Це може обмежити шкоду, спричинену атакою, і допомогти стримати її в певній області мережі.
Регулярні перевірки безпеки	– перегляд політики безпеки; – сканування вразливостей; – тестування на проникнення; – аудит відповідності; – тестування реакції на інцидент.

Продовження таблиці 2.1

1	2
Шифрування конфіденційних даних	– використовувати алгоритми шифрування; – управління ключами – ключі повинні надійно зберігатися та захищені відповідними засобами контролю доступу; – шифрування даних у спокої – для захисту даних у спокої можна використовувати повне шифрування диска або шифрування на рівні файлу. Це гарантує, що навіть якщо зловмисник отримає доступ до фізичного пристрою зберігання даних, він не зможе прочитати дані без ключа шифрування; – шифрування даних під час передачі – можна досягти за допомогою безпечних протоколів зв’язку, таких як SSL/TLS або IPSec. Це гарантує, що навіть якщо зловмисник перехопить мережевий трафік, він не зможе прочитати дані без ключа шифрування; – протоколи обміну ключами – можна досягти за допомогою безпечних протоколів обміну ключами, таких як Diffie-Hellman, RSA тощо.
Заходи контролю доступу	– аутентифікація – використовуйте принаймні багатофакторну автентифікацію; – авторизація – контроль доступу на основі ролей може бути використаний для того, щоб користувачі мали доступ лише до тих даних і ресурсів, які їм необхідні для виконання своїх робочих функцій; – аудит і моніторинг.

Продовження таблиці 2.1

1	2
Методи безпечного кодування	– безпечне зберігання даних – паролі слід хешувати за допомогою надійного алгоритму хешування, такого як bcrypt, а конфіденційні дані мають бути зашифровані як під час передачі, так і під час спокою; – обробка помилок; – безпечний зв'язок – використовуйте TLS/SSL, використовуйте надійні алгоритми шифрування.
Регулярне оновлення програмного забезпечення	– контроль версій – програма повинна регулярно оновлюватися останніми виправленнями безпеки.
План реагування на інцидент	– виявлення та аналіз – використовуйте системи виявлення вторгнень, моніторинг мережевого трафіку або аналіз системних журналів. Метою виявлення та аналізу є виявлення потенційних загроз та оцінка впливу на персональні дані; – стримування та пом'якшення – ізоляція інфікованих систем, відключення скомпрометованих облікових записів або впровадження додаткових заходів безпеки. Метою стримування та пом'якшення є запобігання подальшому пошкодженню персональних даних і обмеження впливу кібератаки; – розслідування та документування – включають аналіз системних журналів, проведення інтерв'ю з персоналом або перегляд мережевого трафіку. Метою розслідування та документування є виявлення першопричини кібератаки та збір доказів для майбутніх правових чи регулятивних заходів; – відновлення та подальше спостереження.

Продовження таблиці 2.1

1	2
Оновлення	– оновити Log4j і OctoberCMS до останньої версії, яка містить патчі для відомих уразливостей.
Впровадити перевірку вхідних даних і кодування вихідних даних	– сувора перевірка вхідних даних для всіх даних користувача, щоб запобігти введенню зловмисних корисних навантажень, таких як атаки XSS або впровадження SQL; – застосовувати вихідне кодування під час відображення створеного користувачем вмісту, щоб запобігти виконанню впроваджених скриптів.

Рекомендації, описані в таблиці 2.1, в основному спрямовані на захист системи від кібератак, таких як WhisperGate і log4j, вразливості OctoberCMS, що дуже важливо, оскільки якщо система добре захищена, важче атакувати дані, які вона містить. Але в той же час, якщо слідувати лише описаним рекомендаціям, є деякі недоліки.

1) Надмірна залежність від технічних рішень: хоча захист мережевої інфраструктури, шифрування конфіденційних даних і впровадження заходів контролю доступу є важливими технічними заходами для захисту особистих даних, їх самих по собі недостатньо. Також важливо враховувати людські фактори, такі як навчання та обізнаність співробітників, щоб забезпечити захист даних від атак соціальної інженерії та внутрішніх загроз.

2) Недостатня увага до конфіденційності: рекомендації щодо протидії кібератакам головним чином зосереджені на безпеці даних і захисту від несанкціонованого доступу. Однак захист особистих даних також вимагає уваги до конфіденційності, наприклад мінімізації даних, політики збереження даних і згоди користувача.

3) Неповний захист: рекомендації щодо протидії кібератакам зосереджені насамперед на запобіганні несанкціонованому доступу до персональних даних. Однак також важливо захистити особисті дані від інших загроз, таких як випадкове розкриття, втрата або знищення. Це вимагає дотримання планів резервного копіювання та відновлення, які, у свою чергу, включають:

– резервне копіювання даних – процес резервного копіювання має бути автоматизованим, щоб забезпечити регулярне резервне копіювання даних, а резервні копії слід періодично тестувати, щоб переконатися, що дані можуть бути успішно відновлені;

– цільовий час відновлення – максимальний час, необхідний для відновлення після втрати даних. RTO слід визначати на основі бізнес-потреб і технічних обмежень, а процеси резервного копіювання та відновлення повинні бути розроблені відповідно до RTO;

– цільова точка відновлення – максимальна кількість втрати даних, яка допустима в разі втрати даних;

– тестування аварійного відновлення – передбачає моделювання аварійного стану для перевірки процесів резервного копіювання та відновлення. Необхідно проводити періодично, щоб переконатися, що процеси резервного копіювання та відновлення ефективні, а RTO та RPO можна досягти.

4) Необхідно встановити надійний процес керування безпекою та конфіденційністю: виконується за допомогою вказівок ISO/IEC 27001 і GDPR. Запровадити політику оновлення програмного забезпечення, щоб забезпечити своєчасне встановлення виправлень, і застосувати SBOM для зменшення ризиків атак на ланцюг поставок;

5) Необхідно визначити потенційні загрози: проводити регулярне тестування безпеки та сканування вразливостей, щоб швидко виявити й усунути потенційні загрози;

6) Необхідно керувати інцидентами безпеки: створити структурований процес реагування на інциденти для ефективного управління та пом’якшення інцидентів безпеки.

3 ЗАСТОСУВАННЯ МОДЕЛЮВАННЯ ЗАГРОЗ ДЛЯ ЗНИЖЕННЯ РИЗИКІВ БЕЗПЕКИ ПІД ЧАС ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Моделювання загроз можна ефективно застосовувати для виявлення потенційних проблем безпеки та конфіденційності та зменшення ризиків безпеки, пов’язаних з обробкою персональних даних. По-перше, всі типи персональних даних, які обробляються, зберігаються або передаються системою, повинні бути визначені, а потім аналіз потоку даних, щоб точно визначити області, де персональні дані можуть бути під загрозою. Наступним кроком є окреслення меж системи, включаючи її компоненти, взаємозв’язки та зовнішні інтерфейси, а також визначення всіх точок входу, через які персональні дані отримуються або передаються.

Вибір відповідної методології загроз також забезпечує структурований підхід до ідентифікації, класифікації та усунення ризиків безпеки, пов’язаних з обробкою персональних даних. Є багато варіантів моделей, таких як STRIDE, PASTA, VAST, OCTAVE і так далі [17]. Модель обирається безпосередньо для вимог системи та конкретних цілей. Потім система оцінюється для виявлення потенційних загроз і вразливостей, пов’язаних з обробкою персональних даних, беручи до уваги можливі вектори атак, несанкціонований доступ, витік даних та інші сценарії, які можуть скомпрометувати персональні дані.

Крім того, необхідно проаналізувати виявлені загрози та вразливі місця, враховуючи їхню ймовірність і вплив на персональні дані. Також необхідно визначити пріоритети ризиків на основі серйозності, щоб ефективно розподілити ресурси та в першу чергу вирішити найбільш критичні ризики. Для усунення виявлених ризиків розроблюються відповідні засоби контролю безпеки та контрзаходи, які можуть включати шифрування, контроль доступу, моніторинг і плани реагування на інциденти, призначені для захисту персональних даних.

Потім створюється вичерпний звіт із детальним описом процесу моделювання загроз, ідентифікованих ризиків і рекомендованих стратегій пом’якшення. Цей звіт дає чітке розуміння ландшафту обробки персональних даних і пов’язаних із цим ризиків безпеки у кваліфікаційній роботі. Перш за все, моделювання загроз є постійним процесом, тому модель загроз слід переглядати та оновлювати в міру

розвитку системи або появи нових загроз, щоб заходи захисту персональних даних залишалися ефективними та актуальними [17].

3.1 Визначення моделі загроз для виявлення загроз конфіденційності

Існує багато методологій моделювання загроз, розглянемо найвідоміші з них в контексті можливого застосування до додатку «Дія».

1) STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege), пропонує системний підхід до моделювання загроз, що дозволяє фахівцям з безпеки аналізувати кожен компонент системи, їх взаємодію та потоки даних. Зосереджуючись на виявленні загроз на етапі проектування, STRIDE допомагає вирішити проблеми безпеки на ранній стадії, зменшуючи ймовірність того, що вразливості будуть використані пізніше. Методологія особливо корисна для веб-додатків, оскільки вона сумісна з діаграмами потоків даних (DFD), забезпечуючи чітку візуалізацію того, як дані рухаються в системі. Ця функція дозволяє фахівцям з безпеки визначити області, де персональні дані можуть бути під загрозою, і розробити цільові стратегії зменшення ризиків [18].

2) PASTA (Process of Attack Modeling and Threat Analysis), ризик-орієнтована методологія, яка фокусується на моделюванні методів зловмисників для виявлення вразливостей. Вона допомагає організаціям краще розуміти потенційні загрози, вразливості та контрзаходи, що дозволяє впроваджувати ефективні стратегії забезпечення безпеки. Складається з семи послідовних етапів [17]. Першим етапом є визначення мети – де визначаються бізнес-цілі, активи та функціональність системи. Другим етапом є визначення технічного середовища – де аналізуються архітектура, технології та конфігурація системи. Третім етапом є виявлення та опис загроз – де виявляються потенційні загрози, їх джерела та можливі вектори атаки. Четвертим етапом є визначення слабких місць – де аналізуються вразливості системи, які можуть бути використані зловмисниками для проведення атак. П’ятим етапом є аналіз ризиків – де оцінюється ймовірність виникнення кожної загрози, а також її можливий вплив на систему та бізнес-цілі. Шостим етапом є розробка контрзаходів – де розробляються стратегії та контрзаходи для зниження ризиків до прийнятного рівня. Контрзаходи можуть включати технічні рішення (наприклад, фаєрволи або шифрування),

процедурні рішення (наприклад, політики безпеки або плани відновлення після аварій) та освітні програми (наприклад, навчання співробітників). Та сьомим етапом є валідація контрзаходів – де після розробки контрзаходів вони повинні бути протестовані та валідовані, щоб переконатися в їх ефективності та доцільності. Це включає перевірку того, чи контрзаходи дійсно знижують ризики, чи не впливають негативно на бізнес-процеси або користувачів, та чи є вони економічно обґрунтованими.

Хоча фокус на оцінці ризиків дуже важливий, він може бути не настільки всеосяжним з точки зору охоплення різних типів загроз, особливо у веб-додатках, де аналіз потоку даних є критично важливим [17].

3) VAST (Visual, Agile, and Simple Threat Modeling – візуальне, гнучке і просте моделювання загроз) – це підхід, покликаний спростити процес моделювання загроз і зробити його більш доступним для неспеціалістів з безпеки. Модель VAST складається з деяких ключових елементів. Першим елементом є візуалізація, де VAST використовує візуальні зображення, такі як діаграми, графіки та схеми, для представлення загроз, вразливостей та контрзаходів. Візуалізація допомагає спрощувати та структурувати інформацію, полегшуючи сприйняття та розуміння складних аспектів інформаційної безпеки. Другим елементом є гнучкість, тому що VAST є гнучкою методологією, яка може бути адаптована до різних типів організацій, систем та додатків. Вона враховує змінність бізнес-вимог, технічного середовища та загроз, дозволяючи проводити постійні оцінки ризиків. Третім етапом є спрощення, ьому що ця модель загроз спрямована на спрощення процесу оцінки ризиків, роблячи його доступним та зручним для різних груп користувачів, включаючи керівництво, співробітників технічного відділу та кінцевих користувачів.

Однак простота цієї моделі може не забезпечити достатнього рівня деталізації при аналізі загроз для веб-додатків, що може призвести до упущення важливих деталей, пов'язаних із захистом персональних даних [17].

4) OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – зосереджується на виявленні критично важливих активів та їхніх вразливостей за допомогою автономного, специфічного для організації підходу. OCTAVE складається з трьох основних фаз [17]. Першою фазою є створення профілю активів та загроз, на цьому етапі залучаються усі зацікавлені сторони, щоб визначити критичні активи

організації та можливі загрози. Важливо враховувати різноманітність загроз, включаючи зовнішні та внутрішні джерела, технічні проблеми, людські помилки та природні катастрофи. Другим етапом є оцінка вразливостей та забезпечення безпеки, на цьому етапі проводиться технічний аналіз системи для виявлення вразливостей та оцінки рівня забезпечення безпеки. Оцінка вразливостей може включати перевірку конфігурацій, аналіз аудиту, тестування на проникнення та інші методи. Останнім етапом є розробка стратегії управління ризиками. На цьому етапі розробляється стратегія управління ризиками, яка враховує результати попередніх етапів. Стратегія може включати вибір контрзаходів для зниження ризиків, планування реагування на інциденти та розробку процедур для моніторингу та оновлення оцінки ризиків.

Хоча OCTAVE корисний для управління організаційними ризиками, він може не підходити для аналізу конкретних загроз для веб-додатків і захисту персональних даних [17].

5) TRIKE – це методологія оцінки ризиків інформаційної безпеки, зосереджена на розробці та аналізі моделей загроз на основі об'єктивних вимог до безпеки. TRIKE розроблено з метою виявлення, аналізу та управління ризиками, пов'язаними з інформаційними активами організації. Існує декілька основних етапів процесу оцінки ризиків за моделлю TRIKE [17]. Першим етапом є визначення вимог до безпеки, де визначаються об'єктивні вимоги до безпеки, які можуть бути засновані на законодавстві, регулятивних вимогах, політиках безпеки або контрактах з клієнтами. Другим етапом є розробка моделі загроз, де на основі визначених вимог до безпеки розробляється модель загроз, яка відображає активи організації, потенційні загрози та вразливості, а також можливі наслідки для організації в разі порушення безпеки. Третім етапом є оцінка ризиків, де аналізується модель загроз, щоб оцінити ймовірність виникнення кожної загрози, її потенційний вплив на активи та загальний рівень ризику. Оцінка ризиків може проводитися за допомогою кількісних або якісних методів, в залежності від потреб організації. Четвертим етапом є розробка стратегії управління ризиками, де на основі результатів аналізу ризиків розробляється стратегія управління ризиками, яка включає вибір контрзаходів для зниження ризиків до прийнятного рівня. Контрзаходи можуть включати технічні рішення, процедурні рішення та освітні програми. Та останнім п’ятим етапом є моніторинг та перегляд, де після розробки та впровадження контрзаходів, організація повинна регулярно

моніторити та переглядати свої системи безпеки, забезпечуючи їх актуальність та ефективність. Моніторинг включає відстеження змін у загрозах, вразливостях та технологічному середовищі, що можуть вплинути на рівень ризику. Процес перегляду забезпечує, що стратегії управління ризиками та контрзаходи залишаються відповідними та ефективними з урахуванням нових загроз та змін у бізнес-процесах.

Хоча ця модель загроз зосереджена на питаннях зацікавлених сторін і відповідальності, підхід TRIKE, заснований на вимогах, може бути не таким ефективним, як STRIDE, для виявлення конкретних загроз веб-додатків і вразливостей потоків даних [17].

Розглянувши ці альтернативні методології моделювання загроз, STRIDE виділяється своїм комплексним характером, структурованим підходом і фокусом на аналізі потоків даних. Його сумісність з діаграмами потоків даних і адаптивність до різних систем, включаючи сучасні веб-додатки, робить STRIDE найкращим вибором для моделювання загроз для веб-додатків і захисту персональних даних [18].

Розглянемо цю модель більш детально.

Модель загроз STRIDE є чудовим вибором для моделювання загроз веб-додатків та захисту персональних даних у них завдяки своїй комплексності, структурованому підходу та широкій застосовності до різних систем [18].

Однією з головних переваг моделі STRIDE є її спрямованість на виявлення загроз на етапі проектування. Такий проактивний підхід допомагає вирішити проблеми безпеки на ранній стадії, зменшуючи ймовірність використання вразливостей у майбутньому. Надаючи пріоритет безпеці з самого початку, веб-додатки «Дія» можуть розроблятися із захистом персональних даних як основною функцією.

Структурована методологія STRIDE дозволяє фахівцям з безпеки систематично оцінювати кожен компонент веб-додатку та його взаємодію з іншими компонентами. Такий цілісний підхід гарантує, що потенційні загрози не залишаться поза увагою, а ризики безпеки будуть належним чином усунені в усій системі. Цей систематичний процес також полегшує документування та передачу результатів, сприяючи співпраці між командами розробників та безпеки. Крім того, сумісність STRIDE з діаграмами потоків даних (DFD) особливо корисна для веб-додатків. DFD забезпечують чітку візуалізацію того, як дані проходять через систему, що полегшує виявлення

потенційних точок вразливості. Використовуючи DFD разом з методологією STRIDE, фахівці з безпеки можуть точно визначити області, де персональні дані можуть бути під загрозою, і розробити цільові стратегії пом'якшення наслідків для захисту конфіденційної інформації [18].

Крім того, адаптивність STRIDE до різних систем, включаючи хмарні і розподілені середовища, робить його універсальним інструментом для моделювання загроз в сучасних веб-додатках. Оскільки веб-додатки продовжують розвиватися і стають все більш складними, гнучкість моделі STRIDE дозволяє їй залишатися актуальною і ефективною у виявленні та зменшенні нових загроз [18].

3.2 Побудова архітектури додатку «Дія»

Перейдемо до побудови моделі загроз додатку «Дія». Архітектура додатку складається з основних компонентів, які можна побачити на рисунку 3.1. Модулі, виділені жовтим кольором, є більш детальним описом того, що використовується в помаранчевих модулях [19].

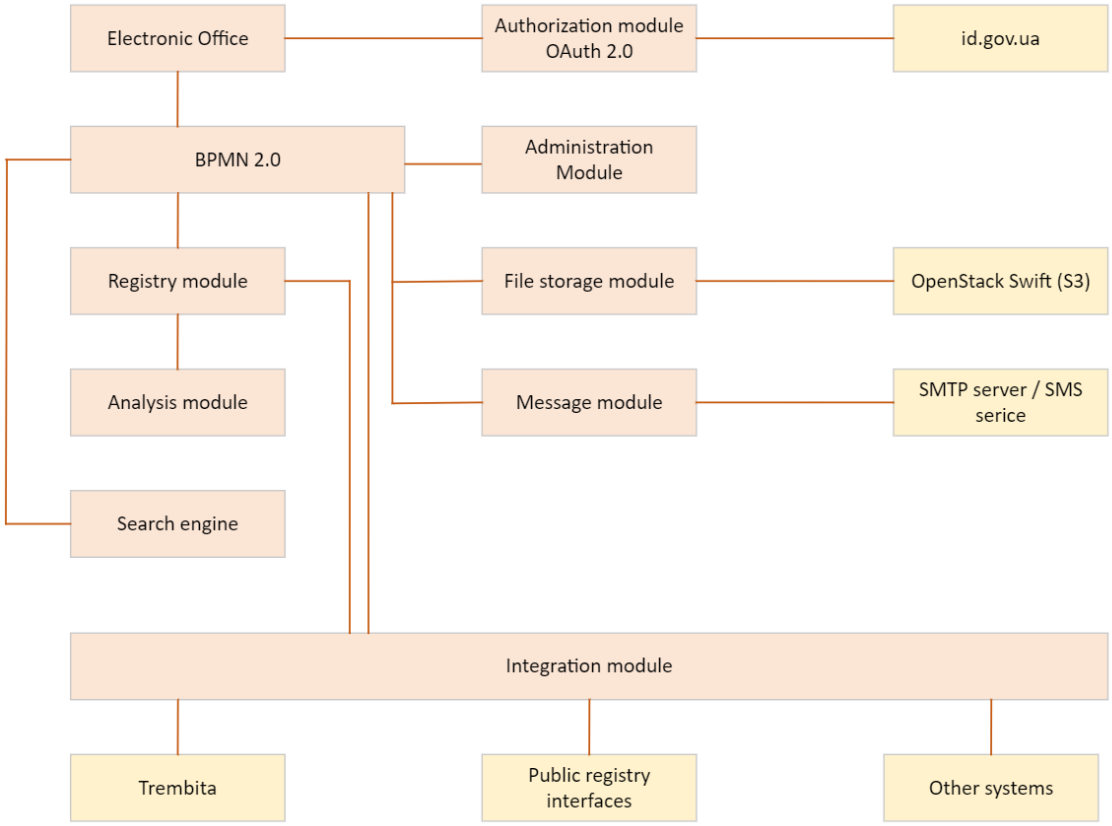


Рисунок 3.1 – Архітектура додатку «Дія»

Нижче більше детально будуть розглянуті основні модулі архітектури.

1) OAuth 2.0 – це відкрита стандартна система автентифікації, яка дозволяє стороннім додаткам отримувати обмежений доступ до ресурсів користувача на іншому сервісі без передачі його облікових даних. Вона дозволяє користувачам надавати дозволи певним додаткам, не розкриваючи свої паролі. OAuth 2.0 пропонує чотири різні моделі авторизації, такі як authorization code, implicit, resource owner password credentials, та client credentials grant, що забезпечують гнучкість для різних сценаріїв використання. Додаток «Дія» використовує OAuth 2.0 як елемент авторизації, а саме Diia.Signature. Для цього реалізовано функціонал авторизації на порталі за допомогою мобільного додатку. Щоб увійти на портал або підписати документ електронним підписом, користувачеві більше не потрібен електронний ключ, який зберігається окремо. Замість цього можна відсканувати QR-код у додатку «Дія» та пройти автентифікацію в мобільному додатку. «Дія.Підпис» також можна використовувати для авторизації на інших державних платформах. Наприклад, сервіс

петицій – це окремий ресурс, користувач заходить і залишається на ньому, а авторизація відбувається через «Дію». Інтеграція OAuth 2.0 забезпечує зручність та безпеку для користувачів, оскільки вони можуть легко надавати доступ до своїх даних на одній платформі, не розкриваючи паролі на інших веб-сайтах. Важливим аспектом OAuth 2.0 є використання токенів доступу, які надаються стороннім додаткам після успішної авторизації користувача. Токени доступу мають обмежений термін дії та можуть бути анульовані будь-коли користувачем. Це забезпечує додатковий рівень контролю та безпеки для користувачів, дозволяючи їм керувати доступом до своїх даних.

OAuth 2.0 також передбачає механізм оновлення токенів, який дозволяє додаткам автоматично оновлювати токени доступу, коли термін їх дії закінчується, без необхідності повторного проходження процесу авторизації користувачем. Це поліпшує зручність використання додатків, оскільки користувачі не повинні постійно надавати дозволи на доступ до своїх даних.

Окрім того, OAuth 2.0 підтримує федеративну авторизацію, яка дозволяє користувачам авторизуватися за допомогою своїх облікових даних від інших сервісів, таких як Google, Facebook або Twitter. Федеративна авторизація полегшує процес реєстрації користувачів на нових сайтах, оскільки вони не повинні створювати нові облікові записи. У цілому, OAuth 2.0 є потужним та гнучким інструментом для авторизації користувачів та керування доступом до ресурсів на різних платформах. Використання OAuth 2.0 у додатку «Дія» та інших державних платформах допомагає забезпечити зручність та безпеку для користувачів, дозволяючи їм легко надавати доступ до своїх даних та контролювати, які додатки можуть використовувати цю інформацію [20].

2) BPMN (Business Process Model and Notation) 2.0 – це графічна нотація для опису та візуалізації бізнес-процесів у стандартизованому форматі. Ця мова специфікації передбачає ряд різних типів діаграм, таких як діаграми процесів, співробітництва, хореографії та розгортання, що дозволяє відображати різні аспекти бізнес-процесів. Додаток «Дія» використовує модуль BPMN 2.0 для налаштування логіки надання послуг. Вона налаштовується бізнес-аналітиками в редакторі BPMN у вигляді діаграм. Тобто архітектуру системи налаштовують розробники, а бізнес-аналітики мають зручний інтерфейс, де вони моделюють процес за допомогою

нотацій. За допомогою BPMN 2.0, компанії можуть легко комунікувати та обмінюватися інформацією про бізнес-процеси між різними підрозділами та сторонніми організаціями. Це полегшує координацію та інтеграцію процесів, забезпечуючи одночасно прозорість та відповідальність. Такий підхід зменшує витрати, допомагає масштабувати систему та досягати поставлених цілей. Не відбувається втручання в основний код системи. Платформа BPMN зберігає дані в реєстрах, взаємодіє з ними, підтягує необхідну інформацію. В основі лежить брокер повідомлень RabbitMQ. Він обробляє чергу повідомлень з реєстрами і гарантує, що процеси не перериваються, а обробляються навіть у разі збоїв при взаємодії із зовнішніми системами. RabbitMQ допомагає забезпечити високу пропускну здатність, надійність та швидке відновлення після збоїв.

У процесі моделювання бізнес-процесів, BPMN 2.0 використовує ряд елементів для представлення дій, подій, ворот, підпроцесів та артефактів. Ці елементи можна легко комбінувати та налаштовувати для відображення складних бізнес-процесів та різних варіантів їх виконання. Таким чином, BPMN 2.0 допомагає бізнес-аналітикам та розробникам легко розуміти та оптимізувати процеси, виявляти та усувати плями в них. Використання BPMN 2.0 у додатку «Дія» дозволяє гнучко підлаштовувати процеси надання послуг та реагувати на зміни у вимогах до реалізації бізнес-процесів. Це також допомагає підвищити ефективність надання послуг та поліпшити якість обслуговування користувачів. Отже, BPMN 2.0 є важливим інструментом для моделювання, аналізу та оптимізації бізнес-процесів, який допомагає спростити співпрацю між різними стейкхолдерами та забезпечити успішну реалізацію проектів у різних організаціях, включаючи додаток «Дія» [20].

3) Модуль адміністрування надає інструменти та функціональність для управління користувачами, послугами та ресурсами платформи. Цей модуль дозволяє адміністраторам додавати, видаляти або змінювати послуги електронного урядування, що надаються платформою. Сюди також входить налаштування інтеграції зі сторонніми організаціями, такими як банки, страхові компанії та інші державні установи. Модуль полегшує управління контентом і ресурсами на платформі, такими як інформаційні сторінки, поширені запитання, оголошення або шаблони документів. Також за допомогою модуля адміністрування здійснюється управління робочими процесами, що включає в себе інструменти для визначення, зміни та моніторингу

різних робочих процесів та процесів, що беруть участь у наданні послуг, такі як BPMN 2.0 або інші інструменти моделювання процесів [20].

4) Модуль зберігання файлів призначений для зберігання, управління та пошуку файлів і документів у системі. Онлайн-сервіси регулярно генерують pdf-файли - заявки, результати. Оскільки файли зберігаються у великих обсягах (понад 500 Гб), вони зберігаються в об'єктному сховищі промислового масштабу – File Storage S3 на базі програмного забезпечення з відкритим вихідним кодом OpenStack. Це сховище забезпечує швидкий доступ до великих файлів, а також можливість резервного копіювання. Сховище є спільним як для порталу, так і для мобільного додатку, а дані зберігаються паралельно [20].

5) Модуль обміну повідомленнями призначений для комунікації між користувачами, адміністраторами та сторонніми сервісами в системі. Ця функція дозволяє користувачам надсилати повідомлення, запити або прохання про підтримку адміністраторам платформи або співробітникам служби підтримки, полегшуючи комунікацію та надаючи допомогу в разі потреби. Модуль обміну повідомленнями також може генерувати автоматичні сповіщення та оповіщення для користувачів, інформуючи їх про статус їхніх запитів на обслуговування, затвердження документів або інші важливі оновлення [20].

6) Модуль реєстру призначений для зберігання, управління та пошуку записів, які зазвичай включають структуровані дані або метадані, в системі. Він зберігає записи, пов'язані з користувачами, послугами та транзакціями в межах платформи. Він також слугує центральним сховищем для доступу до інформації та управління нею, керує дозволами користувачів і правами доступу, гарантуючи, що лише авторизовані користувачі можуть переглядати, редагувати або видаляти певні записи. Це допомагає підтримувати безпеку та захищати конфіденційну інформацію [20].

7) Модуль аналізу призначений для обробки, аналізу та візуалізації даних, пов'язаних з використанням платформи, послугами та продуктивністю, допомагаючи адміністраторам і користувачам приймати обґрунтовані рішення та визначати сфери для вдосконалення. Модуль обробляє і трансформує зібрані дані, готуючи їх до аналізу шляхом агрегування, фільтрації або нормалізації за потреби. Також включає в себе функції для виявлення незвичайних шаблонів або тенденцій в даних,

допомагаючи адміністраторам виявляти потенційні проблеми або проблемні області і вживати коригувальних заходів [20].

8) Пошукова система призначена для того, щоб користувачі могли швидко та ефективно знаходити потрібну інформацію, документи, послуги чи записи в межах платформи. Система обробляє пошукові запити користувачів, інтерпретуючи ключові слова, фрази або інші критерії пошуку, щоб повернути релевантні результати [20].

9) Модуль «Трембіта» функціонує як захищений шлюз, який шифрує та безпечно передає дані між різними державними системами. Однак якість реєстрів та державних ресурсів, з якими він має взаємодіяти, є різною. Хоча новіші системи пропонують API-інтеграцію, обмін даними зі старими системами може бути складним. «Дія» використовує черги повідомлень для асинхронного зв'язку та REST API для синхронного зв'язку. Два основні сервіси полегшують обмін даними: Зовнішній зчитувач та Подія. Сервіс «Зовнішній зчитувач» встановлює безпечні з'єднання із зовнішніми реєстрами, а сервіс «Подія» передає інформацію до інших систем та надсилає сповіщення користувачам. В результаті стає можливою автоматична реєстрація ФОП (приватний підприємець). Зовнішній зчитувач отримує інформацію про користувача з реєстрів та оновлює статус підприємця в Єдиному державному реєстрі. «Дія» безпосередньо спілкується із зовнішнім середовищем через мережу API, оминаючи необхідність у чиновниках [20].

10) Інтерфейси публічних реєстрів – це компоненти, які полегшують доступ та взаємодію з різними державними реєстрами, такими як бази даних, що містять інформацію про підприємства, фізичних осіб або записи про майно. Ці інтерфейси дозволяють користувачам шукати, переглядати та отримувати інформацію з цих реєстрів, забезпечуючи спрощений та зручний спосіб доступу до важливих публічних даних на платформі «Дія» [21].

3.3 Створення моделі загроз для додатку «Дія»

Розібравшись з архітектурою системи, можна перейти до самої моделі загроз. Як було описано раніше, модель загроз базується на моделі загроз STRIDE з використанням програми для побудови моделей. Вигляд створеної моделі загроз можна побачити на рисунку 3.2.

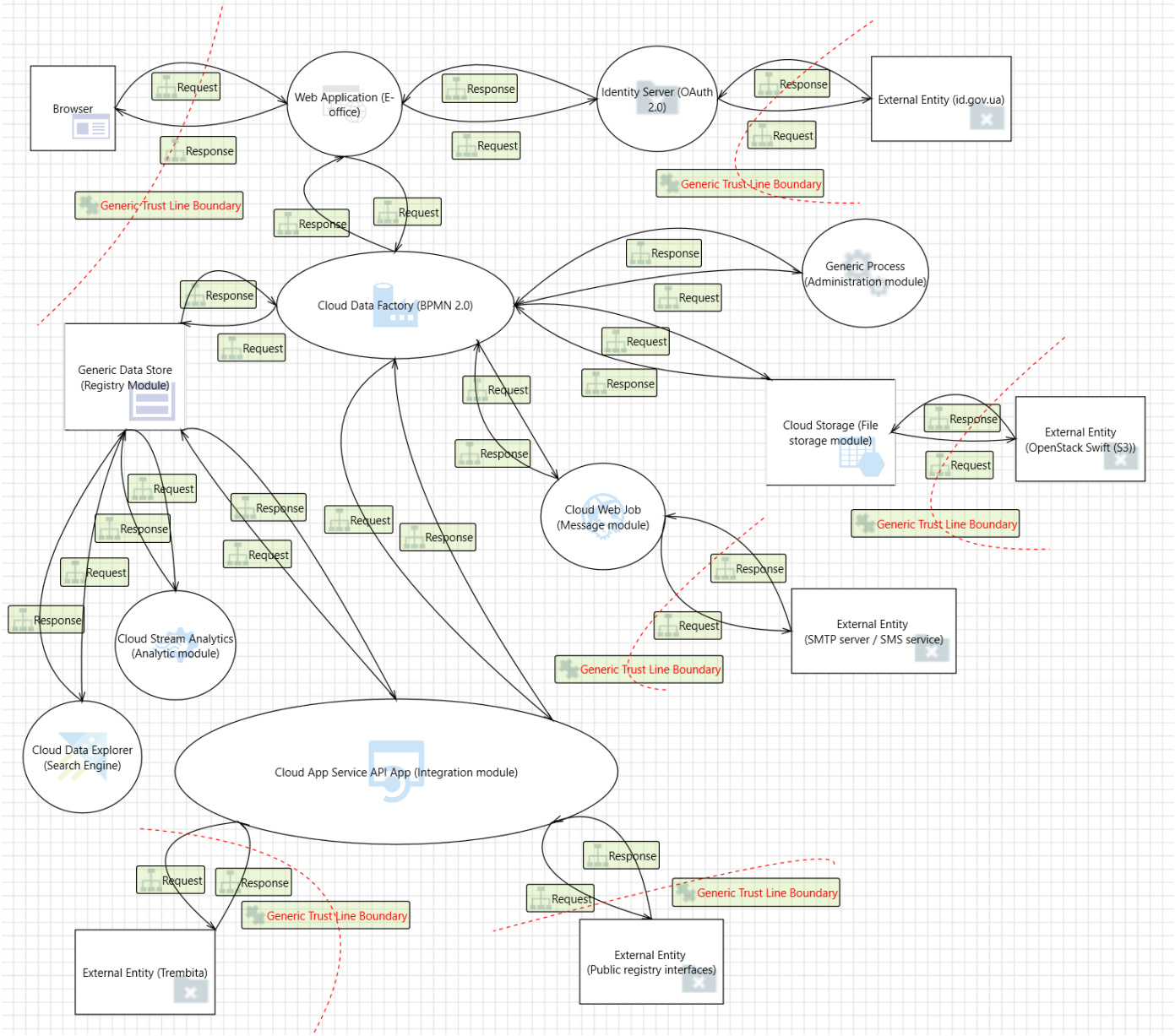


Рисунок 3.2 – Модель загроз для додатку «Дія»

У цій моделі загроз елемент «Браузер» – це програмне забезпечення, яке використовується звичайним користувачем для доступу до системи електронного кабінету. Браузер відповідає за надсилання запитів до системи електронного кабінету та отримання відповідей.

Зв'язок браузера з системою електронного кабінету здійснюється за протоколом HTTPS. Коли користувач вводить URL-адресу або натискає на посилання, браузер надсилає запит на сервер е-кабінету, який містить запитуваний ресурс або дію. Сервер

обробляє запит і надсилає браузеру відповідь, що містить результат запитуваного ресурсу або дії.

Як звичайний користувач, браузер має обмежений доступ до системи електронного кабінету і може виконувати лише певні дії відповідно до ролі та дозволів користувача.

Зі звіту, згенерованого програмою моделювання загроз, для цієї моделі було виявлено загалом 111 вразливостей. Типовий вигляд вразливостей при використанні заданої моделі можна побачити на рисунку 3.3.

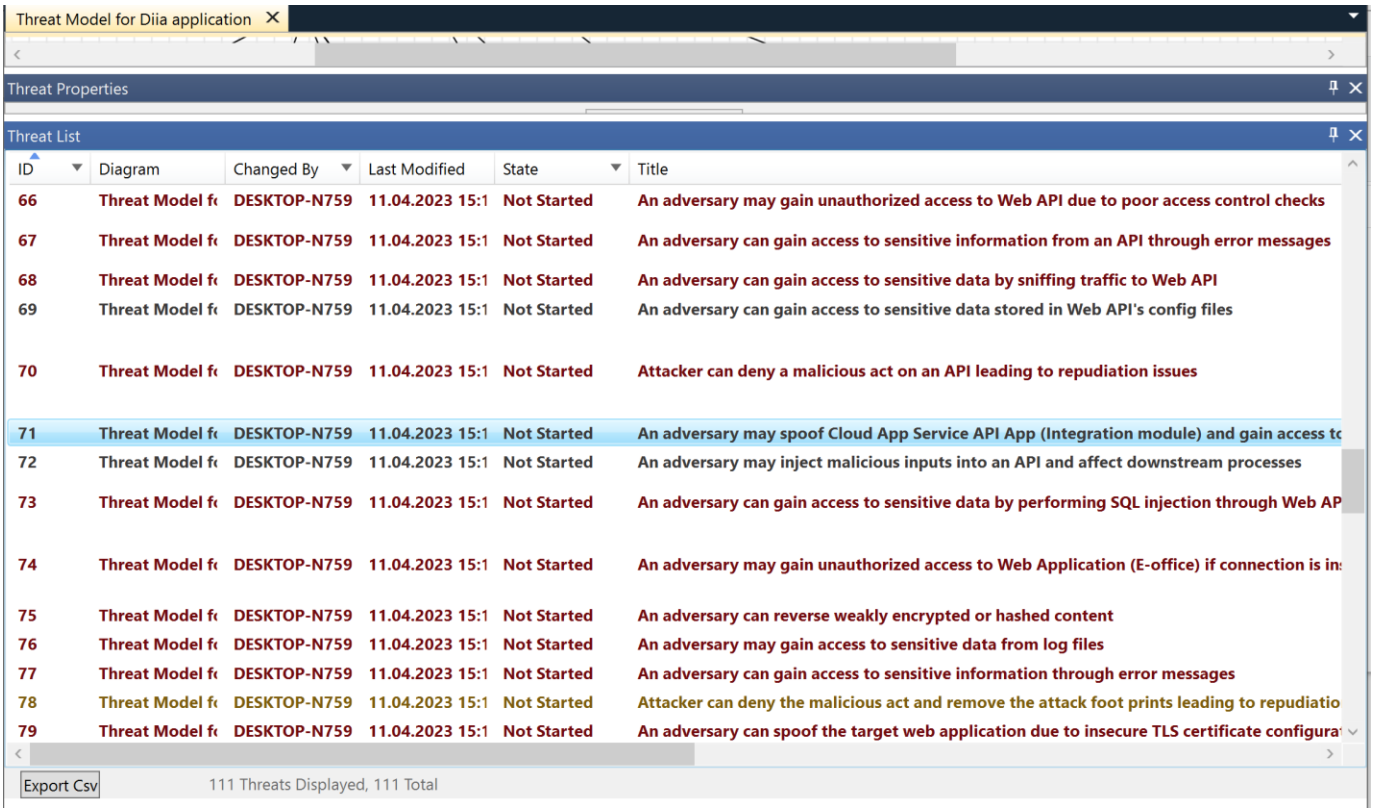


Рисунок 3.3 – Перелік знайдених вразливостей

Згенерований звіт містить опис виявлених потенційних загроз для інформаційної системи, аналіз та оцінку ризиків, що пов'язані з кожною з виявлених загроз, а також рекомендації щодо запобігання та мінімізації наслідків кожної з них.

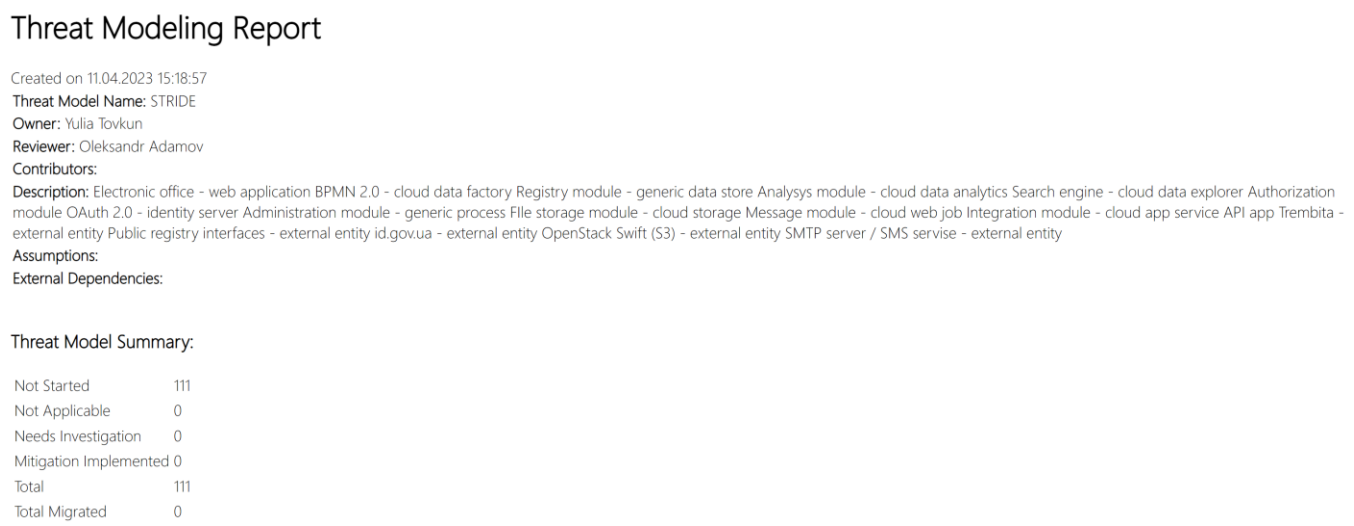
В загальному звіт є цілісним описом моделі STRIDE та допомагає збільшити рівень безпеки інформаційних систем та захистити їх від можливих загроз. Також він включає наступні елементи.

1) Опис інформаційної системи. Звіт включає детальний опис інформаційної системи, включаючи її архітектуру, характеристики, джерела даних, а також важливі функції та операції.

2) Опис виявлених загроз. Звіт містить детальний опис виявлених загроз та їх характеристики з використанням моделі STRIDE. Це включає опис технічних деталей атак, можливі наслідки та інші важливі аспекти, які допоможуть замовнику краще зрозуміти загрози та їх вплив на роботу інформаційної системи.

Звіт після створення моделі загроз STRIDE може бути корисним інструментом для підвищення рівня безпеки інформаційної системи та захисту її від потенційних загроз. Він дозволяє замовнику краще зрозуміти ризики, пов'язані з його інформаційною системою, та вжити заходів для зменшення цих ризиків. Крім того, звіт може бути використаний як основа для подальших заходів з підвищення безпеки інформаційної системи та забезпечення її захисту від потенційних загроз.

Згенерований звіт можна побачити на рисунку 3.4.



Threat Modeling Report

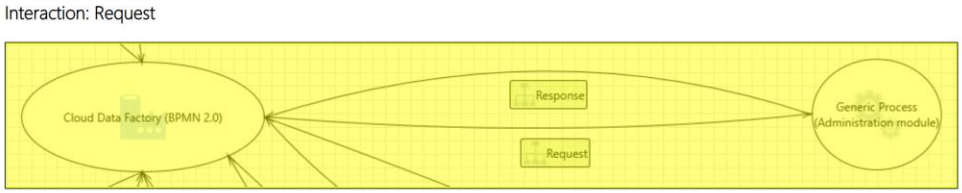
Created on 11.04.2023 15:18:57
Threat Model Name: STRIDE
Owner: Yulia Tovkun
Reviewer: Oleksandr Adamov
Contributors:
Description: Electronic office - web application BPMN 2.0 - cloud data factory Registry module - generic data store Analysys module - cloud data analytics Search engine - cloud data explorer Authorization module OAuth 2.0 - identity server Administration module - generic process FIle storage module - cloud storage Message module - cloud web job Integration module - cloud app service API app Trembita - external entity Public registry interfaces - external entity id.gov.ua - external entity OpenStack Swift (S3) - external entity SMTP server / SMS servise - external entity
Assumptions:
External Dependencies:

Threat Model Summary:

Not Started	111
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	111
Total Migrated	0

Рисунок 3.4 – Звіт про моделювання загроз

Приклади вразливостей, які відображені у звіті можна побачити на рисунку 3.5.



13. An adversary may gain unauthorized access to Generic Process (Administration module) if connection is insecure [State: Not Started] [Priority: High]

Category:	Elevation of Privileges
Description:	An adversary may gain unauthorized access to Generic Process (Administration module) if connection is insecure
Justification:	<no mitigation provided>
Possible Mitigation(s):	It is necessary to partition the network infrastructure to limit the attack surface and limit access to the shared data store. Firewall rules must also be configured to allow only necessary traffic between the cloud data factory and the shared storage, blocking all other traffic. The cloud data factory, the shared data warehouse, and all related software components must be kept up-to-date with the latest security patches to minimize potential attack vectors.
SDL Phase:	Design

Рисунок 3.5 – Приклад виявлених вразливостей за допомогою моделювання загроз

Аналізуючи ці вразливості, було виключено однакові вразливості для різних транзакцій. Кожній вразливості було присвоєно ідентифікатор для подальшої зручності використання. Також були обрані вразливості з високим та середнім пріоритетом, оскільки вони можуть завдати більш серйозної шкоди системі, а згодом і персональним даним. Більш детальний опис цих вразливостей можна знайти в таблиці Б.1 у додатку Б.

Проаналізувавши знайдені вразливості та визначивши їх пріоритетність, можна переходити до розробки рекомендацій щодо їх мінімізації. На основі розглянутих вразливостей були розроблені рекомендації за категоріями загроз та частинами транзакції. Це можна побачити в таблиці Б.2 у додатку Б.

Після того, як рекомендації визначені, їх необхідно застосувати до моделі, щоб можна було побачити, який вплив вони матимуть на безпеку додатку.

Застосування рекомендацій щодо зменшення вразливостей для вразливості під ID 1.6 показано на рисунку 3.6.

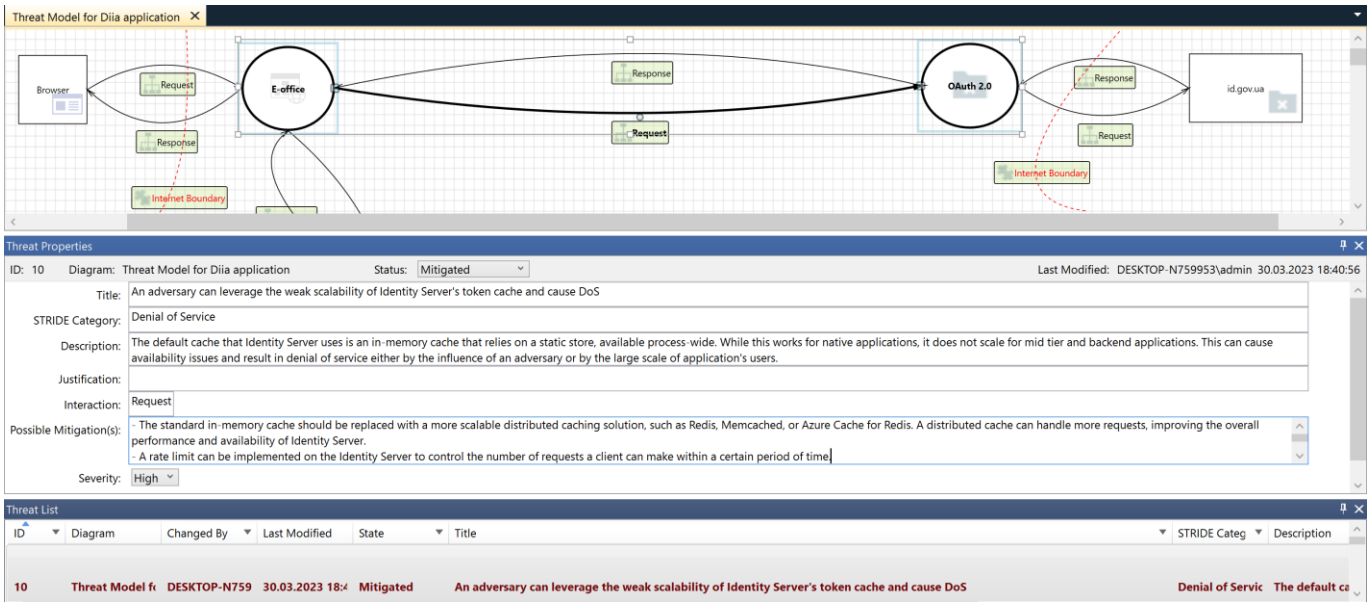
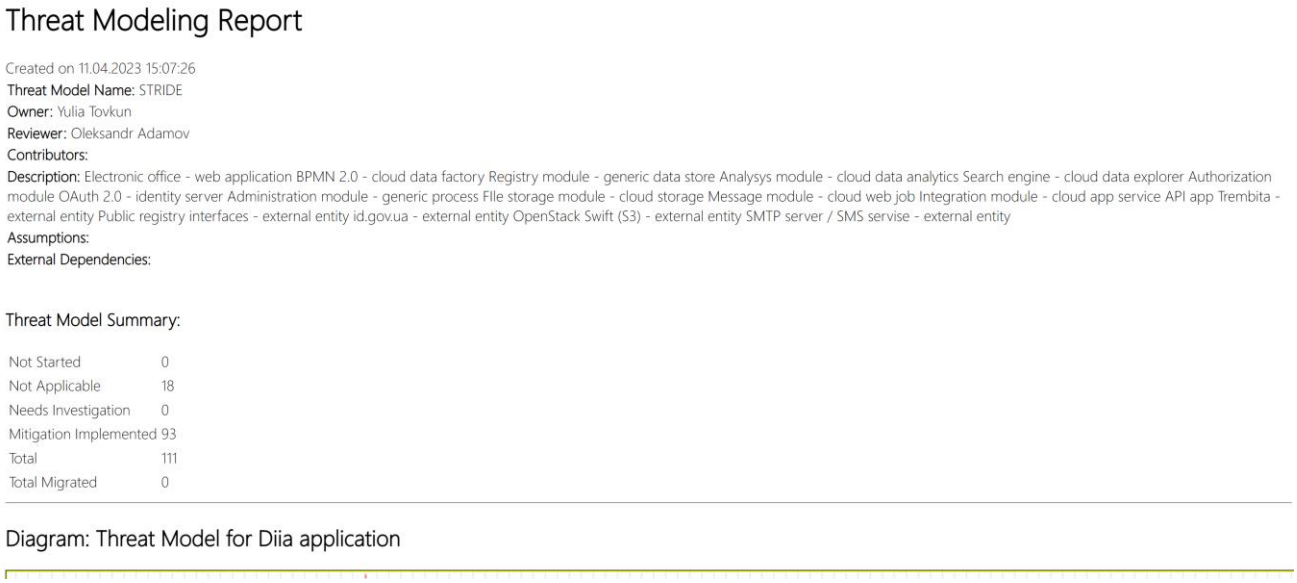


Рисунок 3.6 – Впровадження рекомендацій щодо пом'якшення наслідків в модель загроз

Після застосування рекомендацій щодо пом'якшення наслідків, статистику можна побачити на рисунку 3.7, де показано, що для 93 вразливостей були виконані рекомендації, а 18 були проігноровані (з рівнем суворості нижче середнього).



Threat Modeling Report

Created on 11.04.2023 15:07:26
Threat Model Name: STRIDE
Owner: Yulia Tovkun
Reviewer: Oleksandr Adamov
Contributors:
Description: Electronic office - web application BPMN 2.0 - cloud data factory Registry module - generic data store Analysys module - cloud data analytics Search engine - cloud data explorer Authorization module OAuth 2.0 - identity server Administration module - generic process FIle storage module - cloud storage Message module - cloud web job Integration module - cloud app service API app Trembita - external entity Public registry interfaces - external entity id.gov.ua - external entity OpenStack Swift (S3) - external entity SMTP server / SMS servise - external entity
Assumptions:
External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	18
Needs Investigation	0
Mitigation Implemented	93
Total	111
Total Migrated	0

Diagram: Threat Model for Diia application

Рисунок 3.7 – Звіт про моделювання загроз після усунення наслідків

Таким чином, можна побачити, що модель загроз STRIDE може бути використана для покриття більшості вразливостей в архітектурі додатку «Дія». Далі в роботі буде досліджено ефективність використаної моделі загроз.

4 ОЦІНКА ЕФЕКТИВНОСТІ ПРОАНАЛІЗОВАНИХ МЕТОДІВ ПОМ'ЯКШЕННЯ ЗАГРОЗ, ВИКОРИСТОВУЮЧИ МОДЕЛЬ ОЦІНКИ РИЗИКІВ

Існує багато моделей оцінки ризиків, далі будуть розглянуті найвідоміші з них.

DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability) – це якісна модель оцінки ризиків, яка використовує п'ять критеріїв для оцінки ризику, пов'язаного з вразливістю. Кожен критерій оцінюється за шкалою від 1 до 10, а середній бал використовується для представлення загального ризику. Хоча DREAD простий у використанні, його суб'єктивний характер може призвести до невідповідностей в оцінці, що робить його менш надійним для порівняння ризиків між різними організаціями.

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) – це методологія моделювання загроз, яка класифікує загрози безпеки за шістьма категоріями, зосереджуючись на потенційному впливі на цілісність, конфіденційність та доступність системи. Модель в основному використовується на етапі проектування розробки програмного забезпечення для виявлення та зменшення ризиків. STRIDE не надає числової системи оцінки для визначення пріоритетності ризиків, що може зробити її менш придатною для поточного управління ризиками та порівняння вразливостей.

Common Vulnerability Scoring System (CVSS) v3.1 – це широко визнана і стандартизована система оцінки ризиків, призначена для оцінки загроз безпеці та конфіденційності, що виникають внаслідок виявлених вразливостей. Вона має ряд переваг, таких як узгодженість, порівнянність, комплексні метрики оцінки, адаптивність до конкретних середовищ, широке розповсюдження та підтримка, регулярні оновлення та вдосконалення, а також нейтральність до постачальників.

Ця модель загроз забезпечує послідовну методологію для оцінки вразливостей у програмах, системах і середовищах. Це дозволяє організаціям порівнювати відносну серйозність різних загроз і відповідно розставляти пріоритети в їх усуненні.

CVSS v3.1 також використовує набір чітко визначених метрик для розрахунку базових, часових та оцінок середовища. Ці показники охоплюють різні аспекти

вразливості, включаючи вектор атаки, складність, необхідні привілеї, взаємодію з користувачем, масштаб і вплив на конфіденційність, цілісність і доступність [22].

Оцінка середовища в CVSS v3.1 дозволяє організаціям налаштовувати оцінку на основі своїх унікальних вимог і толерантності до ризиків. Налаштовуючи оцінку середовища, організації можуть визначати пріоритети вразливостей на основі конкретних середовищ, забезпечуючи ефективний розподіл ресурсів [23].

CVSS – це відкритий стандарт, який підтримується Форумом команд реагування на інциденти та безпеки (FIRST). Нейтральність до постачальників гарантує, що його можна застосовувати до будь-якого програмного забезпечення або системи, незалежно від виробника, що дозволяє організаціям послідовно оцінювати та управляти вразливостями у всьому технологічному стеку [22].

В цілому, CVSS v3.1 забезпечує надійну, послідовну та гнучку основу для оцінки загроз безпеці та конфіденційності, що дозволяє організаціям приймати обґрунтовані рішення та ефективно визначати пріоритети для усунення вразливостей [24].

4.1 Визначення рівня ризику до впровадження пом’якшувальних рекомендацій

Використовуючи обрану модель аналізу ризиків CVSS v3.1, розрахуємо ризики за формулами цієї моделі.

Base Score в моделі аналізу ризиків CVSS v3.1 є важливим елементом для визначення потенційних наслідків вразливостей та оцінки загроз для інформаційної системи. Це числова оцінка, яка вказує на серйозність вразливості та наскільки вона може бути небезпечною для системи. Base Score може бути в діапазоні від 0,0 до 10,0, де 10,0 є найвищим значенням. Чим вище значення Base Score, тим серйозніша вразливість та більша ймовірність, що вона може бути використана для атаки на інформаційну систему. Загальний Base Score може бути складним для визначення, тому що він залежить від багатьох факторів. Але завдяки його числовій оцінці, Base Score є корисним інструментом для оцінки ризиків та прийняття рішень щодо заходів з підвищення безпеки інформаційної системи. Він розраховується за формулами (4.1), (4.2) та (4.3).

$$\mathrm{BS} = \frac{\mathrm{E} \cdot \mathrm{I}}{\mathrm{MI}} \cdot 10, \tag{4.1}$$

де BS – base score, агрегована оцінка вразливості, яка враховує exploitability та impact;

E – exploitability, оцінка того, наскільки легко можна скористатися вразливістю;

I – impact, описує максимальний можливий вплив вразливості на систему;

MI – maximum impact, оцінка потенційних наслідків вразливості, якщо її успішно експлуатують.

$$\mathrm{E} = 8.22 \cdot \mathrm{AV} \cdot \mathrm{AC} \cdot \mathrm{PR} \cdot \mathrm{UI}, \tag{4.2}$$

де E – exploitability, числове значення, що відображає, наскільки легко вразливість може бути експлуатована;

AV – attack vector, метрика, що відображає відстань між атакуючим та ціллю атаки;

AC – attack complexity, метрика, яка оцінює, наскільки складно здійснити атаку на вразливість;

PR – privileges required, метрика, що відображає рівень привілеїв, необхідних для успішної експлуатації вразливості;

UI – user interaction, метрика, яка визначає, чи потрібно залучати користувача для успішної експлуатації вразливості.

$$\mathrm{I} = 1 - ((1 - \mathrm{CI}) \cdot (1 - \mathrm{II}) \cdot (1 - \mathrm{AI}), \tag{4.3}$$

де I – impact, числове значення, що відображає потенційні наслідки експлуатації вразливості для системи;

CI – confidentiality impact, метрика, що відображає ступінь компрометації конфіденційної інформації в результаті успішної експлуатації вразливості;

II – integrity impact, метрика, що відображає ступінь порушення цілісності даних або системи в результаті успішної експлуатації вразливості;

AI – availability impact, метрика, що відображає ступінь порушення доступності системи або ресурсів в результаті успішної експлуатації вразливості.

Метрики, що використовуються в цих формулах (вектор атаки, складність атаки, необхідні привілеї, взаємодія з користувачем, вплив на конфіденційність, вплив на цілісність, вплив на доступність), отримують числові значення залежно від їхньої серйозності.

Temporal Score в моделі аналізу ризиків CVSS v3.1 є другим з трьох складових елементів оцінки ризиків та включає в себе додаткову інформацію про вразливість та контекст її використання. Temporal Score може бути в діапазоні від 0,0 до 10,0, де 10,0 є найвищим значенням. Чим вище значення Temporal Score, тим більша ймовірність, що вразливість буде використана для атаки на систему. Temporal Score відображає поточний стан вразливості, враховуючи такі фактори, як наявність експлойтів, патчів та довіру до опису вразливості. Він розраховується за формулою (4.4).

$$TS = BS \cdot ECM \cdot RL \cdot RC, \tag{4.4}$$

де TS – temporal score, числове значення, що відображає вплив часових факторів на оцінку ризику вразливості;

BS – base score, числове значення, що відображає вихідну оцінку ризику вразливості, розраховану на основі метрик Exploitability та Impact;

ECM – exploit code maturity, метрика, що відображає наявність та якість експлойтів для даної вразливості;

RL – remediation level, метрика, що відображає стан наявних виправлень для даної вразливості;

RC – report confidence, метрика, що відображає надійність та точність джерела звіту про вразливість.

Показники, що використовуються у цій формулі (зрілість коду експлойту, рівень виправлення, достовірність звіту), також отримують числові значення залежно від їхньої серйозності.

Environmental Score в моделі аналізу ризиків CVSS v3.1 – це третій елемент оцінки ризиків, який відображає контекст використання вразливості в конкретній інформаційній системі та її середовищі.

Environmental Score відображає конкретний контекст, в якому існує вразливість, враховуючи такі фактори, як вимоги до безпеки постраждалих систем та потенційний вплив. Він розраховується за формулами (4.5), (4.6), (4.7), (4.8).

$$\mathrm{ES} = \mathrm{MBS} \cdot \mathrm{MTS}, \tag{4.5}$$

де ES – environmental score, числове значення, що відображає вплив факторів специфічного середовища на загальну оцінку ризику вразливості;

MBS – modified base score, кориговане значення base score, що відображає оцінку ризику вразливості, з урахуванням специфічних факторів середовища, таких як наявність захисту, наскільки цільова система є критичною та інші аспекти;

MTS – modified temporal score, кориговане значення temporal score, яке враховує специфічні фактори середовища, такі як доступність патчів, зміни в експлуатаційному коді та інші аспекти, що можуть вплинути на оцінку ризику вразливості з часом.

$$\mathrm{MBS} = \frac{\mathrm{ME} \cdot \mathrm{MI}}{\mathrm{MMI}} \cdot 10, \tag{4.6}$$

де ME – modified exploitability, кориговане значення exploitability, яке враховує фактори середовища, такі як наявність захисту, які можуть вплинути на експлуатацію вразливості;

MI – modified impact, кориговане значення impact, яке враховує фактори середовища, такі як важливість цільової системи та інші аспекти, що можуть вплинути на вплив вразливості;

MMI – maximum modified impact, максимальне можливе значення modified impact, що відображає гірший можливий випадок від успішної експлуатації вразливості в даному середовищі.

$$\mathrm{ME} = 8.22 \cdot \mathrm{MAV} \cdot \mathrm{MAC} \cdot \mathrm{MPR} \cdot \mathrm{MUI}, \tag{4.7}$$

де ME – modified exploitability, числове значення, що відображає кориговану оцінку можливості експлуатації вразливості, з урахуванням специфічних факторів середовища;

MAV – modified attack vector, кориговане значення метрики attack vector, яке враховує специфічні фактори середовища, такі як наявність захисту, що може вплинути на відстань атаки;

MAC – modified attack complexity, кориговане значення метрики attack complexity, яке враховує специфічні фактори середовища, такі як наявність контрзаходів, що можуть вплинути на складність атаки;

MPR – modified privileges required, кориговане значення метрики privileges required, яке враховує специфічні фактори середовища, такі як рівень доступу атакуючого, що може вплинути на вимоги до привілеїв для експлуатації вразливості;

MUI – modified user interaction – кориговане значення метрики user interaction, яке враховує специфічні фактори середовища, такі як наявність захисту, що може вплинути на необхідність взаємодії з користувачем для успішної експлуатації вразливості.

$$\mathrm{MI} = (1 - (1 - \mathrm{CR}) \cdot (1 - \mathrm{MCI}))) \cdot (1 - ((1 - \mathrm{IR}) \cdot (1 - \mathrm{MII}))) \cdot \cdot \left(1 - \left((1 - \mathrm{AR}) \cdot (1 - \mathrm{MAI})\right)\right) \cdot 0{,}915, \quad (4.8)$$

де MI – modified impact, кориговане значення impact, яке враховує специфічні фактори середовища, такі як важливість цільової системи та інші аспекти, що можуть вплинути на вплив вразливості;

CI – confidentiality requirement, числове значення, що відображає важливість конфіденційності інформації в даному середовищі;

MCI – modified confidentiality impact, кориговане значення метрики Confidentiality Impact, яке враховує специфічні фактори середовища;

IR – integrity requirement, числове значення, що відображає важливість збереження цілісності інформації в даному середовищі;

MII – modified integrity impact – кориговане значення метрики integrity impact, яке враховує специфічні фактори середовища;

AR – availability requirement, числове значення, що відображає важливість забезпечення доступності інформації в даному середовищі;

MAV – modified availability impact, кориговане значення метрики availability impact, яке враховує специфічні фактори середовища.

Метрикам, що використовуються в цих формулах (модифікований вектор атаки, модифікована складність атаки, модифіковані необхідні привілеї, модифікована взаємодія з користувачем, вимога конфіденційності, вимога цілісності, вимога доступності, модифікований вплив на конфіденційність, модифікований вплив на цілісність, модифікований вплив на доступність), присвоєні числові значення, виходячи з їхньої серйозності [23].

Кожному значенню рядка CVSS v3.1 присвоєно значення, що є ваговим коефіцієнтом та константою, відносно даної моделі, також, для наочності, в таблиці застосовано різні кольорові маркери для кожного параметру моделі ризиків CVSS v3.1, що можна побачити в таблиці 4.1.

Таблиця 4.1 – Числові значення метричних груп з категоріями загроз

Метрична група	Рядкове значення	Числове значення	Рівень загрози з кольоровим маркером
1	2	3	4
Базовий бал			
Вектор атаки (AV)	Мережа (N)	0.85	High
	Суміжна мережа (A)	0.62	Above average
	Місцевий (L)	0.55	Medium
	Фізичний (P)	0.20	Low
Складність атаки (AC)	Низький (L)	0.77	Medium
	Високий (H)	0.44	Low

Продовження таблиці 4.1

1	2	3	4
Потрібні привілеї (PR)	Нічого (N)	0.85	High
	Низький (L)	0.62	Medium
	Високий (H) з незмінним обсягом	0.27	Low
	Високий (H) зі зміненим обсягом	0.50	Low
Взаємодія з користувачем (UI)	Нічого (N)	0.85	Medium
	Потрібно (R)	0.62	Low
Вплив на конфіденційність (C) Вплив на цілісність (I) Вплив на доступність (A)	Нічого (N)	0.0	Low
	Низький (L)	0.22	Medium
	Високий (H)	0.56	High
Тимчасова оцінка			
Зрілість коду експлойту (E)	Не визначено (X)	1.00	High
	Високий (H)	1.00	High
	Функціональний (F)	0.95	Above average
	Підтвердження концепції (P)	0.90	Medium
	Не доведено (U)	0.85	Low
Рівень виправлення (RL)	Не визначено (X)	1.00	High
	Обхідний шлях (W)	0.95	Above average
	Тимчасове виправлення (T)	0.90	Medium
	Офіційне (O)	0.85	Low
	Недоступно (U)	1.00	High
Повідомити про довіру (RC)	Не визначено (X)	1.00	High
	Підтверджено (П)	1.00	High
	Розумний (R)	0.96	Medium
	Невідомо (U)	0.92	Low

Продовження таблиці 4.1

Оцінка середовища			
Вимога конфіденційності (CR) Вимога цілісності (IR) Вимога доступності (AR)	Не визначено (X)	1.00	Above average
	Низький (L)	0.50	Low
	Середній (M)	1.00	Medium
	Високий (H)	1.50	High

Також для зручності можна використовувати калькулятор, розроблений для CVSS v3.1 моделі. Це онлайн інструмент, що дозволяє визначити Base Score, Temporal Score та Environmental Score на основі різних метрик для конкретної вразливості [23].

Для визначення Base Score, калькулятор вимагає вказати характеристики вразливості, такі як доступність виконання атаки, складність виконання атаки, вплив на конфіденційність, доступність та цілісність інформації, а також інші технічні характеристики вразливості. Це можна побачити на рисунку 4.1

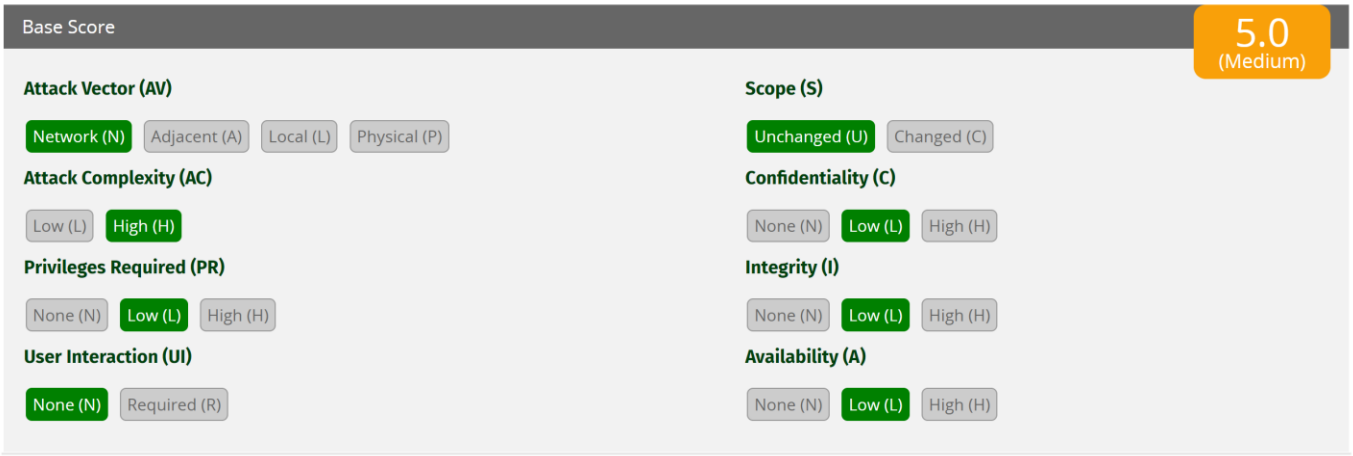


Рисунок 4.1 – Визначення Base Score за допомогою CVSS v3.1 калькулятора

Далі розглянемо застосування моделі оцінки ризиків, а саме Base Score, до створеної моделі загроз для додатку «Дія» без застосування рекомендацій щодо пом'якшення наслідків. Цю модель можна побачити в таблиці 4.2.

Таблиця 4.2 – Оцінка базових ризиків до впровадження пом’якшувальних рекомендацій

ID	Категорія загрози (STRIDE)	Вектор атаки (AV)	Складність атаки (AC)	Необхідні привілеї (PR)	Взаємодія з користувачем (UI)	Сфера застосування (S)	Конфіденційність (C)	Цілісність (I)	Доступність (A)	Базовий бал	Рівень ризику
1	2	3	4	5	6	7	8	9	10	11	12
1.1	Spoofing	Network	Low	None	None	Unchanged	High	High	None	9.1	Critical
1.2		Network	Low	None	None	Changed	High	None	None	8.6	High
1.3		Network	Low	None	Required	Unchanged	High	None	None	6.5	Medium
1.4		Network	High	None	None	Changed	High	High	Low	8.9	High
2.5		Network	High	None	None	Unchanged	High	High	None	7.4	High
2.6		Network	High	Low	None	Unchanged	High	Low	None	5.4	Medium
2.7		Network	High	None	Required	Unchanged	High	Low	None	5.9	Medium
9.9		Network	High	None	Required	Changed	High	High	Low	8.2	High
11.3		Network	High	None	None	Changed	High	High	None	8.7	High
11.4		Network	Low	None	None	Unchanged	High	Low	None	8.2	High
11.5		Network	High	Low	None	Unchanged	High	High	None	6.8	Medium
11.6		Network	High	None	None	Unchanged	High	High	None	7.4	High
2.8	Tampering	Network	High	None	None	Changed	High	High	High	9.0	Critical
2.9		Local	High	Low	None	Changed	High	Low	None	6.4	Medium
9.10		Network	High	None	None	Unchanged	Low	Low	None	4.8	Medium
2.1	Repudiation	Local	High	High	None	Unchanged	None	Low	None	1.9	Low
9.8		Network	Low	None	None	Unchanged	Low	None	None	5.3	Medium
1.5	Information Disclosure	Network	High	None	None	Unchanged	High	High	Low	7.7	High
2.2		Network	High	None	None	Unchanged	High	None	None	5.9	Medium
2.3		Local	Low	Low	None	Unchanged	High	None	None	5.5	Medium

Продовження таблиці 4.2

1	2	3	4	5	6	7	8	9	10	11	12
2.4	Information Disclosure	Network	High	None	None	Unchanged	High	None	None	5.9	Medium
4.3		Network	High	None	None	Unchanged	Low	None	None	3.7	Low
4.4		Network	High	Low	None	Unchanged	Low	None	None	3.1	Low
4.5		Network	High	Low	None	Unchanged	High	None	None	5.3	Medium
7.4		Network	Low	Low	None	Unchanged	High	Low	Low	7.6	High
8.2		Network	Low	None	None	Unchanged	High	Low	Low	8.6	High
8.3		Network	Low	Low	None	Unchanged	High	Low	None	7.1	High
8.4		Adjacent	High	Low	None	Changed	High	High	High	8.0	High
9.3		Adjacent	High	High	Required	Unchanged	High	High	High	6.3	Medium
9.4		Network	High	None	None	Unchanged	Low	Low	Low	5.6	Medium
9.5		Network	High	None	Required	Changed	High	High	Low	8.2	High
9.6		Network	High	Low	None	Unchanged	High	Low	Low	6.4	Medium
9.7		Adjacent	High	None	Required	Unchanged	High	Low	High	6.7	Medium
11.2		Network	High	Low	Required	Unchanged	High	High	Low	6.7	Medium
12.6		Adjacent	High	None	Required	Changed	High	Low	None	6.4	Medium
12.7		Network	High	None	None	Unchanged	Low	Low	Low	5.6	Medium
1.6	Denial of Service	Adjacent	Low	None	None	Unchanged	Low	Low	Low	6.3	Medium
6.3		Network	High	None	None	Unchanged	Low	None	High	6.5	Medium
9.2		Network	High	Low	None	Unchanged	High	Low	Low	6.4	Medium
11.1		Adjacent	Low	None	None	Unchanged	Low	Low	Low	6.3	Medium
3.1	Evaluation of Privilage	Network	High	Low	None	Changed	Low	Low	Low	6.0	Medium
4.1		Adjacent	Low	Low	None	Unchanged	High	Low	Low	6.8	Medium
4.2		Network	High	High	None	Unchanged	High	High	Low	6.2	Medium
5.1		Local	High	High	None	Unchanged	High	Low	Low	5.2	Medium
5.2		Network	Low	High	None	Unchanged	High	High	Low	6.7	Medium
5.3		Network	High	High	None	Changed	High	Low	Low	7.2	High
5.4		Adjacent	High	High	None	Changed	Low	Low	Low	5.1	Medium
5.5		Network	High	High	Required	Unchanged	High	Low	Low	5.3	Medium
5.6		Adjacent	High	Low	Required	Unchanged	High	Low	Low	5.6	Medium

Продовження таблиці 4.2

1	2	3	4	5	6	7	8	9	10	11	12
6.1	Evaluation of Privilage	Network	High	High	None	Changed	High	High	Low	7.9	High
6.2		Network	High	High	None	Changed	High	High	High	8.0	High
7.1		Adjacent	High	Low	None	Changed	High	Low	High	7.9	High
7.2		Adjacent	High	High	None	Unchanged	High	High	High	6.4	Medium
7.3		Adjacent	High	High	Required	Unchanged	High	Low	Low	5.1	Medium
8.1		Network	Low	High	None	Changed	High	High	High	9.1	Critical
9.1		Network	High	High	None	Changed	High	High	High	8.0	High
10.1		Local	High	None	None	Changed	Low	Low	Low	5.6	Medium
12.1		Local	High	Low	None	Changed	Low	Low	Low	5.3	Medium
12.2		Network	High	High	None	Unchanged	High	High	Low	6.2	Medium
12.3		Adjacent	High	High	None	Changed	High	High	Low	7.5	High
12.4		Network	High	High	None	Unchanged	High	Low	High	6.2	Medium
12.5		Network	Low	Low	None	Unchanged	High	Low	Low	7.6	High

Для визначення Temporal Score, калькулятор вимагає вказати характеристики вразливості в контексті, такі як наявність відповідного патча, час публікації вразливості та довіру до інформації щодо вразливості.

Це можна побачити на рисунку 4.2.

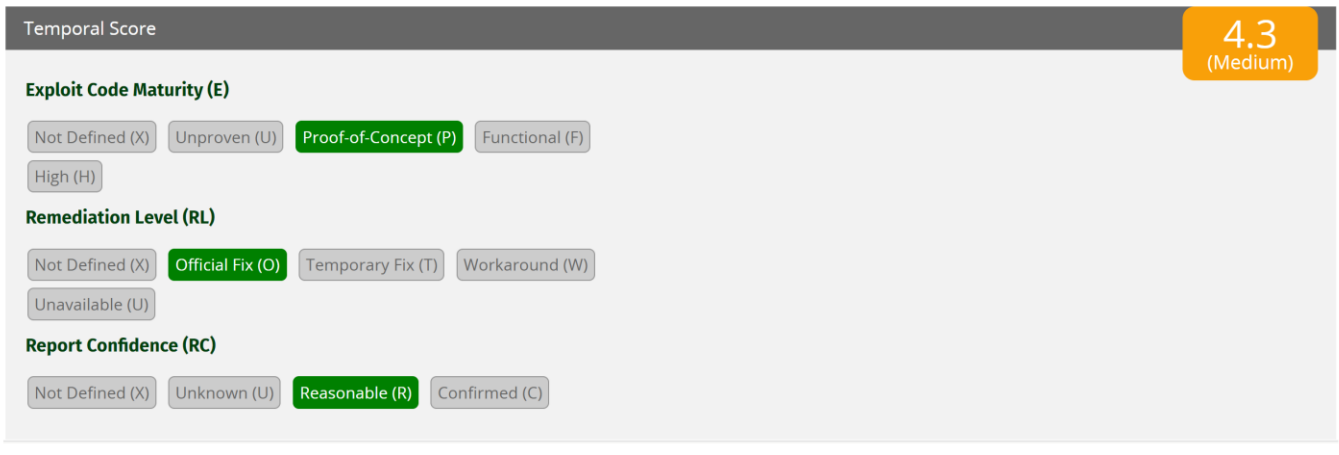


Рисунок 4.2 – Визначення Temporal Score за допомогою CVSS v3.1 калькулятора

Далі розглянемо застосування моделі оцінки ризиків, а саме Temporal Score, до створеної моделі загроз для додатку «Дія» без застосування рекомендацій щодо пом'якшення наслідків. Цю модель можна побачити в таблиці 4.3.

Таблиця 4.3 – Оцінка тимчасових ризиків до впровадження пом’якшувальних рекомендацій

ID	Категорія загрози (STRIDE)	Зрілість коду експлойту (E)	Рівень відновлення (RL)	Повідомити про довіру (RC)	Тимчасова оцінка
1	2	3	4	5	6
1.1	Spoofing	Unproven	Unavailable	Confirmed	8.3
1.2		Unproven	Official Fix	Confirmed	7.5
1.3		Functional	Official Fix	Confirmed	6.0
1.4		Proof-of-Concept	Workaround	Reasonable	7.8
2.5		Proof-of-Concept	Workaround	Reasonable	6.5
2.6		Functional	Temporary Fix	Confirmed	5.5
2.7		High	Official Fix	Confirmed	5.7
9.9		High	Official Fix	Confirmed	7.8
11.3		Unproven	Official Fix	Reasonable	7.3
11.4		Functional	Temporary Fix	Confirmed	7.7
11.5		Functional	Temporary Fix	Confirmed	6.4
11.6		Proof-of-Concept	Temporary Fix	Reasonable	6.5
2.8	Tampering	High	Official Fix	Unknown	7.9
2.9		High	Official Fix	Confirmed	6.1
9.10		High	Official Fix	Confirmed	4.6
2.1	Repudiation	High	Official Fix	Confirmed	1.9
9.8		Functional	Official Fix	Confirmed	4.9
1.5	Information Disclosure	Unproven	Workaround	Reasonable	6.6
2.2		Unproven	Official Fix	Confirmed	5.2
2.3		High	Official Fix	Confirmed	5.3
2.4		Functional	Temporary Fix	Reasonable	5.3
4.3		Proof-of-Concept	Official Fix	Reasonable	3.2
4.4		Proof-of-Concept	Temporary Fix	Reasonable	2.7
4.5		Unproven	Official Fix	Reasonable	4.4
7.4		Proof-of-Concept	Official Fix	Reasonable	6.6
8.2		Proof-of-Concept	Official Fix	Unknown	7.1
8.3		Functional	Workaround	Reasonable	6.5
8.4		Functional	Official Fix	Confirmed	7.4
9.3		Unproven	Unavailable	Confirmed	5.8
9.4		Proof-of-Concept	Temporary Fix	Reasonable	4.9

Продовження таблиці 4.3

1	2	3	4	5	6
9.5	Information Disclosure	Functional	Official Fix	Confirmed	7.6
9.6		Unproven	Official Fix	Reasonable	5.4
9.7		Proof-of-Concept	Temporary Fix	Confirmed	6.1
11.2		High	Workaround	Reasonable	6.3
12.6		Functional	Official Fix	Unknown	5.5
12.7		Proof-of-Concept	Official Fix	Confirmed	5.1
1.6	Denial of Service	Unproven	Workaround	Confirmed	5.6
6.3		High	Official Fix	Confirmed	6.2
9.2		Functional	Workaround	Confirmed	6.1
11.1		Proof-of-Concept	Temporary Fix	Reasonable	5.5
3.1	Evaluation of Privilage	Proof-of-Concept	Official Fix	Confirmed	5.4
4.1		Functional	Workaround	Reasonable	6.2
4.2		High	Official Fix	Confirmed	5.9
5.1		High	Official Fix	Confirmed	5.0
5.2		Proof-of-Concept	Workaround	Confirmed	6.2
5.3		High	Official Fix	Confirmed	6.9
5.4		Unproven	Official Fix	Reasonable	4.3
5.5		Proof-of-Concept	Official Fix	Confirmed	4.8
5.6		High	Temporary Fix	Reasonable	5.2
6.1		Unproven	Official Fix	Confirmed	6.9
6.2		High	Official Fix	Confirmed	7.6
7.1		Proof-of-Concept	Official Fix	Confirmed	7.1
7.2		Functional	Temporary Fix	Reasonable	5.8
7.3		High	Official Fix	Confirmed	4.9
8.1		High	Official Fix	Confirmed	8.7
9.1		Proof-of-Concept	Temporary Fix	Reasonable	7.0
10.1		High	Official Fix	Confirmed	5.4
12.1		Proof-of-Concept	Workaround	Reasonable	4.7
12.2		Functional	Official Fix	Reasonable	5.5
12.3		High	Official Fix	Confirmed	7.2
12.4		Proof-of-Concept	Official Fix	Reasonable	5.4
12.5		Unproven	Official Fix	Confirmed	6.6

Для визначення Environmental Score, калькулятор вимагає вказати контекст використання вразливості, такі як важливість активів, які можуть бути пошкоджені, доступність зловмисників до інформаційної системи та їхні знання та навички. Це можна побачити на рисунку 4.3.

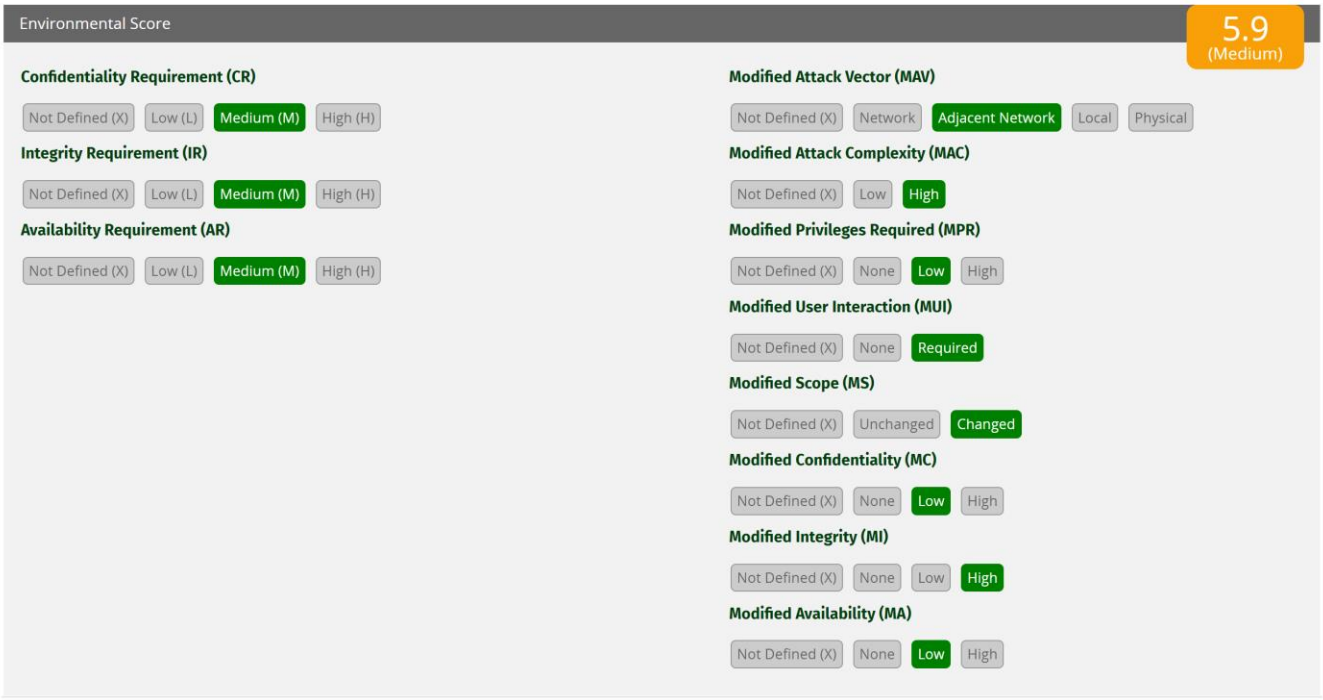


Рисунок 4.3 – Визначення Environmental Score за допомогою CVSS v3.1 калькулятора

Далі розглянемо застосування моделі оцінки ризиків, а саме Environmental Score, до створеної моделі загроз для додатку «Дія» без застосування рекомендацій щодо пом'якшення наслідків. Цю модель можна побачити в таблиці 4.4.

Таблиця 4.4 – Оцінка ризиків середовища до впровадження пом’якшувальних рекомендацій

ID	Категорія загрози (STRIDE)	Вимога конфіденційності (CR)	Вимога цілісності (IR)	Вимога доступнот (AR)	Модифікій вектор атаки (MAV)	Модифікована складність атаки (MAC)	Потрібні змінені привілеї (MRP)	Модифікована взаємодія з користувачем (MUI)	Змінена сфера застосування (MS)	Модифікована конфіденційність (MC)	Модифікована цілісність (MI)	Модифікована доступність (MA)	Оцінка середовища
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.1	Spoofing	High	High	Medium	Network	Low	None	None	Unchanged	High	High	None	9.0
1.2		Medium	Medium	Low	Network	Low	None	None	Changed	High	None	None	8.2
1.3		Medium	Medium	Low	Network	Low	None	Required	Unchanged	High	None	None	6.0
1.4		High	High	Medium	Network	High	None	None	Changed	High	High	Low	8.0
2.5		High	High	Medium	Network	High	None	None	Unchanged	High	High	None	7.1
2.6		High	Medium	Low	Network	High	Low	None	Unchanged	High	Low	None	6.8
2.7		High	Medium	Low	Network	High	None	Required	Unchanged	High	Low	None	7.0
9.9		High	High	Medium	Network	High	None	Required	Changed	High	High	Low	8.0
11.3		High	High	Medium	Network	High	None	None	Changed	High	High	None	7.0
11.4		High	Medium	Low	Network	Low	None	None	Unchanged	High	Low	None	9.0
11.5		High	High	Low	Network	High	Low	None	Unchanged	High	High	None	7.0
11.6		High	High	Low	Network	High	None	None	Unchanged	High	High	None	7.1
2.8	Tampering	Medium	Medium	Low	Network	Low	None	None	Changed	High	High	High	8.8
2.9		High	High	Medium	Local	High	Low	None	Unchanged	High	Low	None	7.3
9.10		Medium	Medium	Low	Network	High	None	None	Unchanged	Low	Low	None	4.6
2.1	Repudiation	Low	Medium	Low	Local	High	High	None	Unchanged	None	Low	None	1.9
9.8		Medium	High	Low	Network	Low	None	None	Unchanged	Low	None	None	5.7
1.5	Information Disclosur	Medium	Low	Low	Network	High	None	None	Unchanged	High	High	Low	5.9
2.2		High	Low	Low	Network	High	None	None	Unchanged	High	None	None	4.0

Продовження таблиці 4.4

1	2	3	4	5	6	7	8	9	10	11	12	13	14
2.3	Information Disclosure	High	Low	Low	Local	Low	Low	None	Unchanged	High	None	None	7.9
2.4		High	Low	Low	Network	High	None	None	Unchanged	High	None	None	6.9
4.3		Medium	Low	Low	Network	High	None	None	Unchanged	Low	None	None	3.2
4.4		High	Medium	Medium	Network	High	Low	None	Unchanged	Low	None	None	3.3
4.5		High	Low	Medium	Network	High	Low	None	Unchanged	High	None	None	5.9
7.4		Medium	Low	Medium	Network	Low	Low	None	Unchanged	High	Low	Low	6.3
8.2		Medium	Low	Low	Network	Low	None	None	Unchanged	High	Low	Low	6.7
8.3		Low	Low	Low	Network	Low	Low	None	Unchanged	High	Low	None	4.7
8.4		High	Medium	Medium	Adjacent	High	Low	None	Changed	High	High	High	7.5
9.3		High	High	Medium	Adjacent	High	High	Required	Unchanged	High	High	High	5.8
9.4		Medium	Medium	Medium	Network	High	None	None	Unchanged	Low	Low	Low	4.9
9.5		High	Medium	Low	Network	High	None	Required	Changed	High	High	Low	7.8
9.6		Medium	Medium	Low	Network	High	Low	None	Unchanged	High	Low	Low	6.8
9.7		Medium	Low	Medium	Adjacent	High	None	Required	Unchanged	High	Low	High	6.9
11.2		Medium	Low	Low	Network	High	Low	Required	Unchanged	High	High	Low	6.9
12.6		Medium	Medium	Medium	Adjacent	High	None	Required	Changed	High	Low	None	5.5
12.7		Medium	Low	Medium	Network	High	None	None	Unchanged	Low	Low	Low	5.4
1.6	Denial of Service	Medium	Medium	Medium	Adjacent	Low	None	None	Unchanged	Low	Low	Low	5.6
6.3		Medium	Medium	Medium	Network	High	None	None	Unchanged	Low	None	High	6.2
9.2		High	Medium	Medium	Network	High	Low	None	Unchanged	High	Low	Low	7.1
11.1		Medium	Medium	Medium	Adjacent	Low	None	None	Unchanged	Low	Low	Low	5.5
3.1	Evaluation of Privilage	Medium	Medium	Medium	Network	High	Low	None	Changed	Low	Low	Low	5.4
4.1		High	Medium	Medium	Adjacent	Low	Low	None	Unchanged	High	Low	Low	7.2
4.2		Medium	Medium	Medium	Network	High	High	None	Unchanged	High	High	Low	5.9
5.1		Medium	Medium	Medium	Local	High	High	None	Unchanged	High	Low	Low	5.0
5.2		High	High	Medium	Network	Low	High	None	Unchanged	High	High	Low	6.6
5.3		High	Low	Low	Network	High	High	None	Changed	High	Low	Low	7.6
5.4		Medium	Medium	Medium	Adjacent	High	High	None	Changed	Low	Low	Low	4.3

Продовження таблиці 4.4

1	2	3	4	5	6	7	8	9	10	11	12	13	14
5.5		Medium	Medium	Medium	Network	High	High	Required	Unchanged	High	Low	Low	4.8
5.6		Medium	Medium	Medium	Adjacent	High	Low	Required	Unchanged	High	Low	Low	5.2
6.1		Medium	Medium	Medium	Network	High	High	None	Changed	High	High	Low	6.9
6.2		Medium	Medium	Medium	Network	High	High	None	Changed	High	High	High	7.7
7.1		Medium	Medium	Medium	Adjacent	High	Low	None	Changed	High	Low	High	7.1
7.2		High	High	Medium	Adjacent	High	High	None	Unchanged	High	High	High	5.8
7.3		High	Medium	Medium	Adjacent	High	High	Required	Unchanged	High	Low	Low	5.9
8.1		High	High	High	Network	Low	High	None	Changed	High	High	High	8.7
9.1		Medium	Medium	Medium	Network	High	High	None	Changed	High	High	High	7.1
10.1		Medium	Medium	Medium	Local	High	None	None	Changed	Low	Low	Low	5.4
12.1		Medium	Medium	Medium	Local	High	Low	None	Changed	Low	Low	Low	4.7
12.2		Medium	Medium	Medium	Network	High	High	None	Unchanged	High	High	Low	5.5
12.3		Medium	Medium	Medium	Adjacent	High	High	None	Changed	High	High	Low	7.2
12.4		Medium	Medium	Medium	Network	High	High	None	Unchanged	High	Low	High	5.4
12.5		Medium	Medium	Medium	Network	Low	Low	None	Unchanged	High	Low	Low	6.6

На основі створеної моделі ризику можна розрахувати середнє значення ризику та нанести його на графік, використовуючи базовий бал. Середнє значення ризику без застосування рекомендацій по пом'якшенням, можна побачити у таблиці 4.5.

Таблиця 4.5 – Середнє значення ризику без застосування рекомендацій по пом'якшенням

Threat category	Average risk value without mitigations
Spoofing	75,91
Tampering	63,30
Repudiation	36,00
Information Disclosure	63,31
Denial of Service	63,75
Evaluation of Privileges	65,86

Графік відповідно до вище наведеної таблиці можна побачити на рисунку 4.4.

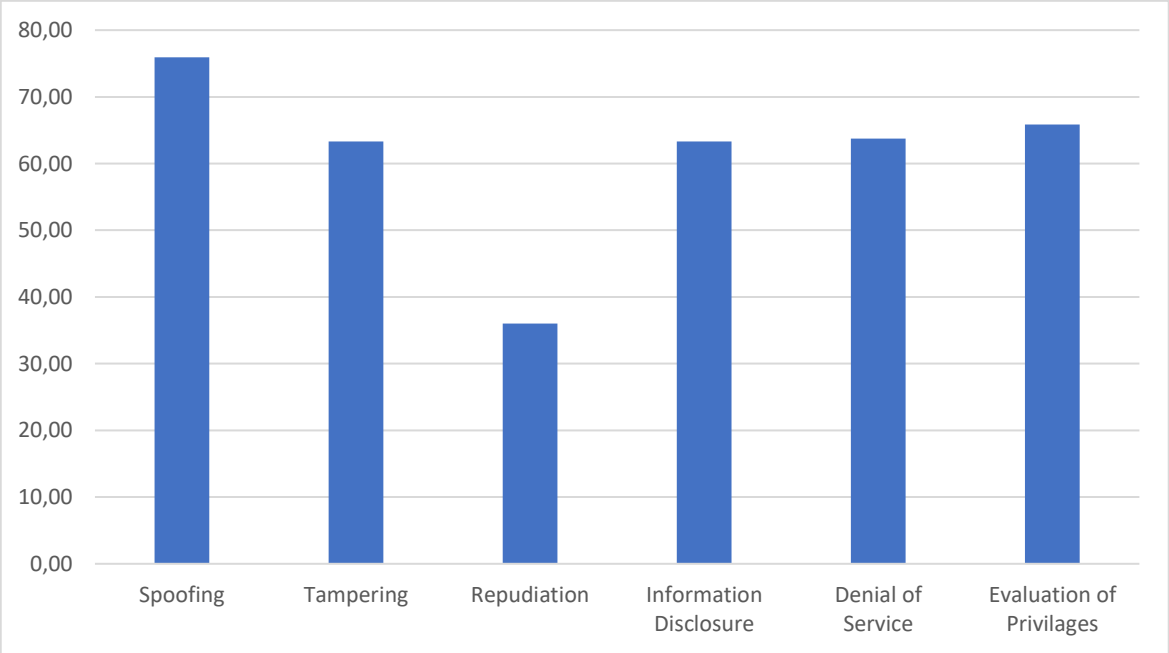


Рисунок 4.4 – Графік значень ризиків для кожної категорії

На представленому вище графіку, який базується на розрахунку рівнів ризиків для вразливостей, знайдених за допомогою моделі загроз STRIDE, видно розподіл різних видів ризиків у відповідних категоріях. Модель STRIDE включає шість ключових категорій загроз: Спуфінг, Тамперінг, Неповноважений доступ, Відмова в обслуговуванні, Виявлення та Елевація привілеїв.

З графіка видно, що найбільша кількість ризиків високого рівня виявлена у категорії «Спуфінг».

Спуфінг – це атака, коли зловмисник намагається видати себе за іншу особу або систему, щоб отримати доступ до конфіденційних даних або зробити шкоду. Це може включати такі види атак, як електронний лист зі спуфінгом, фішинг, атаки на DNS та інші.

Детальний аналіз графіка також демонструє, що інші категорії також мають певні ризики, хоча у меншому масштабі. Це підкреслює необхідність комплексного підходу до забезпечення кібербезпеки, який враховує всі можливі вектори атак.

4.2 Визначення рівня ризику після впровадження пом’якшувальних рекомендацій

Далі розглянемо ризики з рекомендаціями щодо їх зниження, де ризик знижується до мінімуму після застосування рекомендацій. Пом’якшувальні рекомендації можна побачити у таблиці Б.2 в додатку Б.

Після застосування ризиків нижчого рівня для кожного з типів атак моделі CVSS v3.1, типи ризиків можна побачити в таблиці 4.6.

Далі розглянемо ризики з рекомендаціями щодо їх зниження де ризик стає мінімальним після впровадження цих рекомендацій, розроблених після моделювання загроз. Пом'якшувальні рекомендації можна побачити у таблиці Б.2 в додатку Б. Вони були розроблені з метою зменшення рівня ризику та підвищення захищеності додатку «Дія» та персональних даних користувачів.

Після впровадження рекомендацій щодо зниження ризиків для кожного з типів атак, відповідно до моделі оцінки ризиків CVSS v3.1, ми можемо спостерігати зміни у характеристиках ризиків. Оновлені типи ризиків із врахуванням впроваджених рекомендацій можна переглянути у таблиці 4.6.

Таблиця 4.6 – Мінімальне значення ризику для кожного вектору атаки та типу рахунку

Вектор атаки (AV)	Тип оцінки	Значення ризику
1	2	3
Мережа	Базова оцінка	2.7 (Low)
	Тимчасова оцінка	2.2 (Low)
	Оцінка середовища	2.5 (Low)
Суміжні	Базова оцінка	2.4 (Low)
	Тимчасова оцінка	2.0 (Low)
	Оцінка середовища	2.2 (Low)
Локальний	Базова оцінка	2.3 (Low)
	Тимчасова оцінка	1.9 (Low)
	Оцінка середовища	2.1 (Low)

Після проведення аналізу таблиці Б.1, яка містить інформацію про виявлені вразливості та відповідні значення ризиків, можна побудувати таблицю 4.7. Вона враховує загальну кількість векторів атак для кожного типу загроз згідно з моделлю STRIDE. Таким чином, таблиця 4.7 дає змогу отримати детальніше уявлення про характеристики вразливостей та кількість атак, які можуть бути спрямовані на кожен з типів загроз.

Таблиця 4.7 – Обсяг вразливостей для кожної категорії загроз

Категорія загрози	Масштаб вразливостей
Спуфінг	Мережеві вразливості – 12
Фальсифікація	Мережеві вразливості – 2, Локальні вразливості – 1
Відмова	Мережеві вразливості – 1, Локальні вразливості – 1
Розкриття інформації	Мережеві вразливості – 14, Суміжні вразливості – 4, Локальні вразливості – 1
Відмова в обслуговуванні	Мережеві вразливості – 2, Суміжні вразливості – 2
Оцінка привілеїв	Мережеві вразливості – 12, Суміжні вразливості – 7, Локальні вразливості – 3

Продовжуючи аналіз, для кожного типу вразливості, обчислюється середнє значення ризику, яке ґрунтується на базових балах, визначених у моделі CVSS v3.1. Враховуючи рекомендації щодо зниження ризиків, представлені в таблиці Б.1 додатку Б, можна побудувати таблицю 4.8, яка відображає середнє значення ризику для кожного типу вразливості з урахуванням запропонованих заходів.

Таблиця 4.8 – Середнє значення ризику з урахуванням рекомендацій

Категорія загрози	Середнє значення ризику з урахуванням пом'якшувальних рекомендацій
Спуфінг	27,00
Фальсифікація	25,66
Відмова	25,00
Розкриття інформації	26,15
Відмова в обслуговуванні	25,50
Оцінка привілеїв	25,50

На рисунку 4.5 представлений графік, який демонструє порівняння значень ризиків з врахуванням рекомендацій щодо зменшення ризиків та без них. Цей графік допомагає візуально оцінити вплив запропонованих рекомендацій на зниження рівня ризику для кожного типу вразливості, виявлених за допомогою моделі загроз STRIDE.

Рисунок 4.5 містить дві групи стовпчиків для кожного типу вразливості, а саме:

– стовпчики зі значеннями ризиків без застосування рекомендацій;

– стовпчики зі значеннями ризиків з урахуванням рекомендацій.

Таким чином, рисунок 4.5 наглядно відображає ефективність застосування рекомендацій для зниження рівня ризику, дозволяючи оцінити, наскільки успішно ці рекомендації допомагають зменшити потенційні загрози для персональних даних користувачів та стабільності додатку «Дія». Це сприяє кращому розумінню важливості впровадження таких рекомендацій та можливих наслідків у випадку неврахування цих заходів.

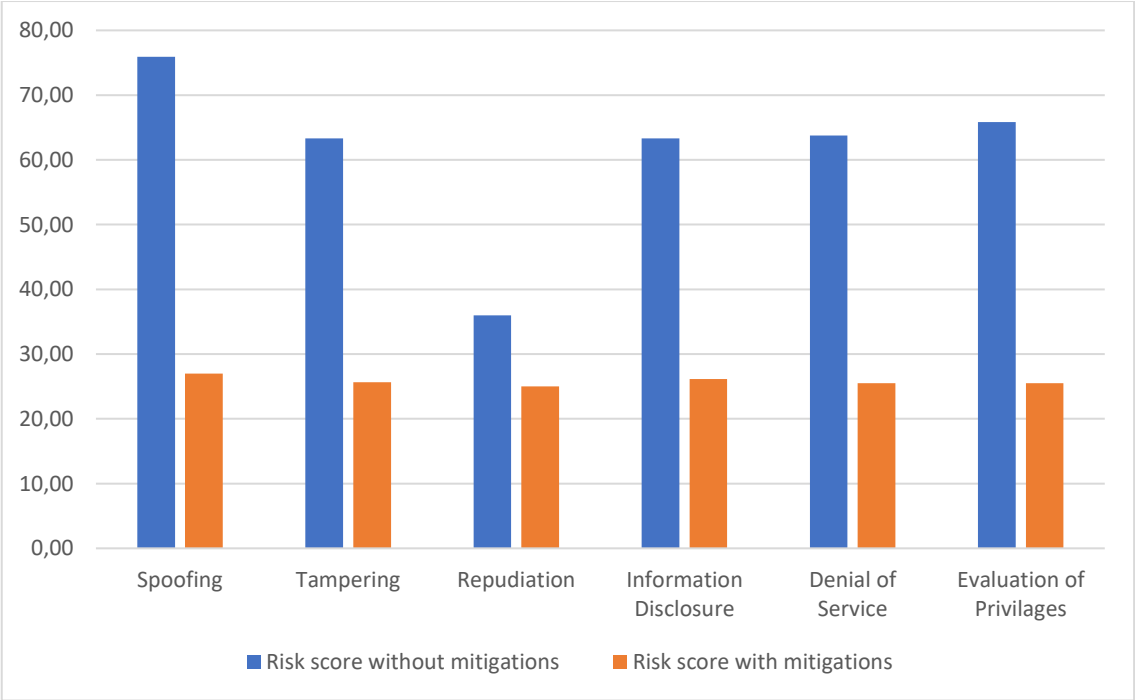


Рисунок 4.5 – Порівняння рівня ризику з урахуванням пом'якшувальних рекомендацій та без них

З урахуванням отриманих даних, можна відзначити позитивні зміни у рівні ризику після впровадження розроблених рекомендацій щодо зменшення вразливостей. Виявлені ризики, які раніше становили серйозну загрозу для персональних даних користувачів та надійності додатку «Дія», в результаті ретельної роботи над покращенням захисту та безпеки, стають мінімальними та не мають значного впливу на функціонування застосунку.

У процесі дослідження, було використано систему оцінки вразливостей CVSS v3.1, яка дозволила провести об'єктивний аналіз та класифікацію потенційних ризиків. Застосування цієї моделі допомогло краще зрозуміти характеристики кожної вразливості, визначити їх серйозність та спрогнозувати можливі наслідки. Відповідно, це забезпечило можливість розробити ефективні рекомендації, спрямовані на мінімізацію рівня ризику та підвищення безпеки додатку.

Враховуючи ці аспекти, можна стверджувати, що впровадження розроблених рекомендацій на основі дослідження і аналізу з допомогою CVSS v3.1 моделі справді забезпечило значне зниження рівня ризику для персональних даних користувачів та стабільності додатку «Дія». Це підкреслює важливість не тільки самого науково-обґрунтованого підходу до питань кібербезпеки, але й використання надійних методів для оцінки та моніторингу ризиків.

ВИСНОВКИ

У ході магістерської роботи було розроблено пропозиції щодо підвищення рівня захисту персональних даних у контексті кібервійни. Задля цього, було проведено дослідження, спрямоване на виявлення законодавчих вимог для пом'якшення загроз безпеки та конфіденційності, захисту персональних даних відповідно до українського законодавства та GDPR, а також аналіз кіберінцидентів та вразливостей системи «Дія».

В результаті дослідження було виявлено, що українське законодавство має певні недоліки в порівнянні з вимогами GDPR, які можуть створювати додаткові загрози конфіденційності та безпеки персональних даних громадян.

Також було проаналізовано кібератаку на платформу «Дія», в ході якої було виявлено критичні вразливості системи та запропоновано рекомендації щодо зберігання персональних даних для запобігання подібних атак в майбутньому.

Використовуючи методи моделювання загроз, було розроблено модель загроз на основі моделі STRIDE для виявлення загроз конфіденційності та проаналізовано архітектуру додатку «Дія» з метою зниження ризиків безпеки під час обробки персональних даних.

Оцінка ефективності проаналізованих методів пом'якшення загроз недоторканності приватного життя з точки зору ризиків безпеки та конфіденційності була здійснена за допомогою моделі оцінки ризиків CVSS v3.1, яка дозволила виявити слабкі сторони та області для поліпшення.

На підставі проведеного дослідження, рекомендується вдосконалити українське законодавство щодо захисту персональних даних, наближаючи його до вимог GDPR, а також розробити та впровадити комплекс заходів щодо підвищення рівня безпеки персональних даних, зокрема на платформі «Дія». Серед таких заходів можна виділити наступні.

1) Регулярний аналіз та оновлення законодавства в сфері захисту персональних даних, з метою адаптації до сучасних технологій та міжнародних стандартів [25].

2) Впровадження системи регулярного моніторингу та аудиту захисту персональних даних на платформі «Дія» та інших аналогічних ресурсах.

3) Організація та проведення навчань та тренінгів для спеціалістів, які працюють з персональними даними, з метою підвищення їхньої компетентності та освіченості в сфері кібербезпеки та захисту персональних даних.

4) Розробка та впровадження стратегії реагування на кіберінциденти, яка передбачає швидке виявлення та усунення вразливостей, відновлення роботи системи та повідомлення громадян про можливі порушення їхньої конфіденційності.

5) Використання моделі загроз, розробленої в ході цієї магістерської роботи, для планування та реалізації заходів щодо забезпечення безпеки персональних даних на платформі.

В цілому, впровадження зазначених рекомендацій сприятиме підвищенню рівня безпеки та конфіденційності персональних даних в Україні, а також зміцненню довіри громадян до системи «Дія» та інших аналогічних сервісів.

Окремі результати роботи були представлені та опубліковані на декількох конференціях. Перша робота була висвітлена на всеукраїнській науково-практичній Internet-конференції «Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті» і опублікована за її підсумками [1]. Друга робота була представлена на II всеукраїнській студентській науковій конференції «Експериментальні та теоретичні дослідження в контексті сучасної науки» і опублікована за підсумками цієї конференції [8]. Третя робота була висвітлена на III міжнародній науковій конференції «Наукові тренди постіндустріального суспільства» і опублікована за її підсумками [9]. Четверта робота опублікована у збірнику міжнародного молодіжного форуму [25].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Товкун Ю. І. Зв'язок кібератак із наземними бойовими діями. *Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті* : матеріали Всеукраїнської науково-практичної Internet-конференції, м. Харків, 15 – 16 лист. 2022 р. Харків : ХНАДУ, 2022. С. 65 – 67.

2. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 15.03.2023).

3. Закон України "Про захист персональних даних". URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 15.03. 2023).

4. Закон України "Про інформацію". URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.03. 2023).

5. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text (дата звернення: 15.03. 2023).

6. Наказ "Про затвердження документів у сфері захисту персональних даних". URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення: 15.03. 2023).

7. General Data Protection Regulation. URL: https://gdpr-info.eu/ (дата звернення: 15.03. 2023).

8. Товкун Ю. І. Аналіз Основних Ризиків при Впровадженні GDPR. *Експериментальні та теоретичні дослідження в контексті сучасної науки* : матеріали II Всеукраїнської студентської наукової конференції, м. Івано-Франківськ, 24 берез. 2023 р. Вінниця : ГО «Європейська наукова платформа», 2023. С. 51 – 52.

9. Товкун Ю. І. Аналіз атаки на державні органи України із застосуванням фреймворку METASPLOIT. *Наукові тренди постіндустріального суспільства* : матеріали III Міжнародної наукової конференції, м. Дніпро, 21 жовт. 2022 р. Вінниця : ГО «Європейська наукова платформа», 2022. С. 130 – 131.

10. Destructive malware targeting Ukrainian organizations. URL:

https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (дата звернення: 04.04. 2023).

11. Cyberattacks are Prominent in the Russia-Ukraine Conflict. URL: https://www.trendmicro.com/es_es/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html (дата звернення: 04.04. 2023).

12. Звідки хакери взяли персональні дані 2 млн українців. URL: https://dou.ua/lenta/articles/inquiry-about-diia-data-leak/ (дата звернення: 04.04. 2023).

13. Атака на українські урядові сайти через вразливість. URL: https://ain.ua/2022/01/14/ataku-na-ukrayinski-sajty-mogly-provesty-cherez-cms/ (дата звернення: 04.04. 2023).

14. Фрагмент дослідження кібератак 14.01.2022. URL: https://cert.gov.ua/article/18101 (дата звернення: 04.04. 2023).

15. Analysis of WhisperGate. URL: https://www.nioguard.com/2022/01/analysis-of-whispergate.html (дата звернення: 04.04. 2023).

16. An overview of Russia's cyberattack activity in Ukraine. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (дата звернення: 04.04.2017).

17. Security Modeling and Threat Modeling. URL: https://blog.51sec.org/2018/10/threat-modeling.html (дата звернення: 10.04. 2023).

18. Microsoft Threat Modeling Tool – STRIDE. URL: https://blog.51sec.org/2022/11/microsoft-threat-modeling-tool-stride_15.html (дата звернення: 10.04. 2023).

19. «Дія» під капотом. URL: https://ain.ua/ru/2021/08/18/diya-god-spustya-v-kitsoft-rasskazali-pro-avtomatizirovannye-uslugi-i-novye-tehnologii-na-portale/ (дата звернення: 10.04. 2023).

20. Розробка порталу "Дія". URL: https://ain.ua/ru/2020/06/30/kak-v-kitsoft-razrabatyvali-diya/ (дата звернення: 10.04. 2023).

21. Threat Modeling Process. URL: https://owasp.org/www-community/Threat_Modeling_Process#stride-threat-list (дата звернення: 10.04. 2023).

22. Common Vulnerability Scoring System v3.1: User Guide. URL: https://www.first.org/cvss/user-guide (дата звернення: 17.04. 2023).

23. What Is CVSS v3.1. URL: https://www.mend.io/resources/blog/cvss-v3-1/ (дата звернення: 17.04. 2023).

24. Salini P., Kanmani S. Survey and analysis on Security Requirements Engineering. *Computers & Electrical Engineering*. 2012. № 6. – P. 1785–1797. – URL: https://www.sciencedirect.com/science/article/abs/pii/S0045790612001644?via%3Dihub (дата звернення: 18.04.2023)

25. Товкун Ю. І. До питання проблем захисту персональних даних на території України у порівнянні із GDPR. *Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій* : матеріали 25-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь у XXI столітті», м. Харків, 20 – 21 квіт. 2021 р. Харків : ХНУРЕ, 2021. С. 52 – 53.