Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Розробка політики безпеки, моделей загроз та критеріїв захисту інформаційного ресурсу AllTransUA

Виконав(ла): студент(ка) 4 курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Завадський К. С. (прізвище та ініціали)

Керівник (підпис) Оробчук О. Р. (прізвище та ініціали)

Нормоконтроль (підпис) (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н. В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
20_24__

Міністерство освіти і науки України

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

(повна назва факультету)

Кафедра кібербезпеки

(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н. В.
(підпис) (прізвище та ініціали)
« » 20_24__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня **Бакалавр**

(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека

(шифр і назва спеціальності)

студенту Завадському Костянтину Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи Розробка політики безпеки, моделей загроз та критеріїв захисту інформаційних ресурсів

Керівник роботи Оробчук Олександра Романівна, доктор філософії

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

Затверджені наказом ректора від «*10*» *квітня* 20_24__ року №

.

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Моделі безпеки, моделі загроз та аналіз критеріїв захисту Інформаційних ресурсів, функціонал сайту AllTransUA

4. Зміст роботи (перелік питань, які потрібно розробити)

1. Моделі безпеки (Дискреційна, мандатна та рольова політики безпеки)

2. Підходи до побудови моделі загроз (STRIDE, TRIKE, OCTAVE, PASTA, VAST)

3. Критерії оцінки захищеності інформаційних систем (Критерії цілісності, доступності, автентичності, спостережності, гарантій)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці			
Безпека в надзвичайних ситуаціях			

7. Дата видачі завдання 29.01.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Вибір теми для дослідження		
2	Затвердження теми кваліфікаційної роботи бакалавра		
3	Розробка завдання на кваліфікаційну роботу бакалавра, складання календарного плану КРБ		
4	Затвердження завдання завідувачем кафедри		
5	Опрацювання літературних джерел і складання плану КРБ		
6	Збирання фактичних матеріалів під час проєктно-технологічної практики		
7	Збирання фактичних матеріалів під час досліджень за темою КРБ		
8			
9			
10			
11			
12			
13			
14			
15			
16			

Студент _____ (підпис) Завадський К. С. (прізвище та ініціали)

Керівник роботи _____ (підпис) Оробчук О. Р. (прізвище та ініціали)

АНОТАЦІЯ

Розробка політики безпеки, моделей загроз та критеріїв захисту інформаційного ресурсу AllTransUA // Кваліфікаційна робота ОР «Бакалавр» // Завадський Костянтин Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2024 // С. 85, рис. – 33, табл. – 1 , кресл. – 10 , додат. – 1.

КЛЮЧОВІ СЛОВА: Політики Безпеки, Модель Загроз, Критерії, Конфіденційність, Цілісність, Доступність, Спостережність.

Кваліфікаційна робота бакалавра містить теоретичний виклад моделей побудови політики безпеки, моделей загроз, їхній аналіз та практичну реалізацію за обраною однією з технологій на прикладі аналізу стану безпеки інформаційного транспортного ресурсу AllTransUA. Мета виконання кваліфікаційної роботи бакалавра полягає в проектуванні моделі безпеки для вказаного вище інформаційного ресурсу та підвищенні безпеки інформаційного ресурсу та зменшенні імовірності виникнення наявних загроз безпеці інформаційних ресурсів, а саме трьом основним поняттям – конфіденційність, цілісність та доступність. Згідно з результатами досліджень, було розроблено низку рекомендацій щодо зменшення імовірності виникнення зовнішніх та внутрішніх загроз.

ABSTRACT

Development of security policy, threat model and protection criteria of information source AllTransUA // Thesis of educational level "Bachelor"// Zawadskyi Kostiantyn Serhiyovich // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group CB-41 // Ternopil, 2024 // P. 85, fig. - 33, tab. - 1, chair. - 10, added. – 1.

Keywords: Security Policy, Threat Model, Criteria, Confindentiality, Integrity, Availability, Observability.

Bachelor’s qualification work contains theoretical representation of creating safety policy models, threat models, their analysis and practical realization by choosing one of following technologies by example of analyzing safety state of information public transport source called AllTransUA. The purpose of doing following bachelor’s qualification work is projecting information source’s safety model and decreasing risk of available information security threats, and namely, three main concepts – confidentiality, identity and authentity. According to research results, there were developed a number of recommendations of lowering the risk of external and internal threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

НСД	—	несанкціонований доступ
ПБ	—	політика безпеки
ДПБ	—	дискреційна політика безпеки
МПБ	—	мандатна політика безпеки
РПБ	—	рольова політика безпеки
КЦД	—	конфіденційність, цілісність, доступність
СУІБ	—	система управління інформаційною безпекою
КД	—	довірча конфіденційність
КА	—	адміністративна конфіденційність
КО	—	повторне використання об’єктів
КК	—	аналіз прихованих каналів
КВ	—	конфіденційність при обміні
ЦД	—	довірча цілісність
ЦА	—	адміністративна цілісність
ЦО	—	відкат
ЦВ	—	цілісність при обміні
ДР	—	використання ресурсів
ДС	—	стійкість до відмов
ДЗ	—	гаряча заміна
ДВ	—	відновлення після збоїв
НР	—	реєстрація
НИ	—	ідентифікація та автентифікація
НК	—	достовірний канал
НО	—	розподіл обов’язків
НЦ	—	цілісність комплексу засобів захисту
НТ	—	самотестування

НВ	—	ідентифікація та автентифікація при обміні
НА	—	автентифікація відправника
НП	—	автентифікація отримувача
КЗЗ	—	комплекс засобів захисту
КС	—	комп’ютерна система
АС	—	автоматизована система
СЗІ	—	система захисту інформації
SDLC	—	життєвий цикл розробки програмного забезпечення

ВСТУП

Одними з найважливіших складових для безперервності безпеки функціонування інформаційних ресурсів є розробка політик за моделями безпеки, розробка моделі загроз та порушника, встановлення критеріїв оцінки захищеності інформаційної системи.

Основною метою розробки політик безпеки є насамперед впровадження стандартів, правил та вимог щодо визначення, виявлення, попередження та зниження ризиків безпеки, а також для створення базової концепції впровадження та розробки методів із забезпечення персоналу належним рівнем безпеки.

Політики безпеки поділяються на три види: дискреційну, мандатну та рольову і характеризуються такими поняттями як суб'єкти та об'єкти доступу, мітки секретності, користувачі та ролі.

Розробка моделі загроз спрямована на надання персоналу розуміння щодо необхідних для задіювання засобів захисту та контролю в конкретних випадках, аналіз профілю зловмисника та векторів атак (активів, що представляють собою предмет інтересу зловмисників), щоб власники інформаційних ресурсів були ознайомлені з перерахованими загрозами та готові до вжиття відповідних заходів при настанні загроз з ціллю уникнення заподіяних збитків для інформаційних ресурсів. Завдання розробки моделі порушника полягає в визначенні зовнішніх, внутрішніх порушників, їхніх мотивів та заходів щодо ліквідацій загрози з їхнього боку.

Серед найбільш поширених підходів до побудови моделей безпеки розрізняють STRIDE, TRIKE, OCTAVE, PASTA та VAST.

Завдання розробки критеріїв оцінки захищеності інформаційних ресурсів полягають в визначенні вимог щодо захисту інформаційних ресурсів від несанкціонованого доступу (надалі – НСД); створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки

захищеності інформації в комп’ютерних системах і їх відповідності встановленим вимогам.

В кваліфікаційній роботі бакалавра буде проведено аналіз всіх вище згаданих політик, моделей безпеки, моделей загроз та критеріїв безпеки для обраного інформаційного ресурсу і розробки їх з урахуванням виду інформації, що циркулює в інформаційному ресурсі, а також встановлено висновки про відповідність інформаційно-пізнавального транспортного порталу AllTransUA критеріям оцінки захищеності та розроблено на їхній основі рекомендації для зменшення ризику загроз та задоволення всіх вимог з Критеріїв оцінки захищеності інформаційних ресурсів.

1 МЕТОДИ ПОБУДОВИ ПОЛІТИКИ БЕЗПЕКИ, МОДЕЛІ ЗАГРОЗ ТА КРИТЕРІЇВ ОЦІНКИ ЗАХИЩЕНОСТІ

Інформаційні технології (надалі – ІТ) стали невід'ємною складовою нашого повсякденного життя, яка охоплює всі галузі діяльності. Вони значно змінюють спосіб нашої роботи, навчання, спілкування та розваг. У бізнесі ІТ сприяють автоматизації процесів, підвищенню ефективності та покращенню взаємодії з клієнтами. В галузі освіти вони гарантують доступ до безмежних ресурсів знань, інтерактивного та дистанційного навчань [1]. В контексті медицини ІТ допомагають у діагностиці, лікуванні та моніторингу здоров'я пацієнтів [2]. Окрім того, інформаційні технології змінюють наш спосіб організації дозвілля завдяки доступу до різноманітних розваг, соцмереж та інших цифрових платформ [3]. Таким чином, ІТ-технології сприяють покращенню якості життя та відкривають нові можливості в кожній галузі нашої діяльності і в даній роботі буде показано їхню користь саме під час проєктування, вдосконалення та використання сайтів.

1.1 Теоретичні відомості про політики та моделі безпеки

Одними з найбільш широкодосліджених політик вважаються три типи – дискреційна, мандатна та рольова політики безпеки. Якщо перші дві вважаються давно відомими та добре дослідженими, то остання з них була розроблена завдяки нещодавнім науковим досягненням в галузі захисту інформації [4, с. 104].

В цьому підрозділі буде детально описано кожен з трьох типів моделей побудови політики безпеки.

2.2.6 Дискреційна політика безпеки

Дискреційна політика безпеки (ДПБ) передбачає розмежувальне керування доступом на основі:

- однозначної ідентифікації суб’єктів та об’єктів;
- визначення прав доступу суб’єкта до об’єкта системи за певними зовнішніми відносно системи правилами.

Матрицю доступу для розробки ДПБ можна сформувати двома різними способами, зокрема через листи можливостей (кожному суб’єкту створюється перелік усіх об’єктів, доступних даному суб’єкту) та листи контролю над доступом (кожному об’єкту відповідає список суб’єктів, яким доступний цей об’єкт). Ця політика є однією з найбільш поширених в світі і ставиться за замовчуванням в усіх системах [4, с. 104];

1.1.2 Мандатна політика безпеки

Мандатна (повноважна) політика безпеки (надалі – МПБ) полягає в мандатному керуванні доступом (Mandatory Access Control – MAC), яке передбачає:

- Визначення решітки конфіденційності інформації;
- Присвоєння рівня конфіденційності кожному об’єктові системи;
- Задоволення вимог ідентифікованості до кожного з суб’єктів та об’єктів системи;

Найкраще дану ПБ описує модель Белла-Ла-Паддула, яка гарантує отримання суб’єктом доступу до інформації лише за умови наявності достатніх для цього повноважень, і що жоден суб’єкт (окрім системного адміністратора) не зможе здійснювати перенесення даних між об’єктами з вищого рівня конфіденційності в нижчий.

МПБ має значно прозоріші та зрозуміліші правила в порівнянні з ДПБ, окрім того, системи, побудовані на цій ПБ, є захищенішими в порівнянні з тою ж ДПБ. Проте така політика безпеки чинить високі навантаження на обчислювальні ресурси [5].

1.1.3 Рольова політика безпеки

Рольова політика безпеки (надалі – РПБ) є самостійною ПБ і базується на ДПБ, слугуючи її розвитком. Згідно РПБ права доступу суб'єктів формулюються відповідно до їхніх повноважень та обов'язків (ролей).

Рольова політика безпеки є доволі гнучкою і активно використовується в мережевих ОС, великих системах керування БД та всюди, де чітко встановлені права та повноваження адміністраторів та користувачів інформаційної системи. На основі цієї ПБ можна реалізовувати інші різні політики, наприклад, МПБ [6].

2.2Моделі загроз та підходи до формування моделі безпеки

Серед найбільш поширених методологій побудови моделі загроз розрізняють наступні: STRIDE, TRIKE, OCTAVE, PASTA, VAST. В цьому пункті розглянемо коротко особливості кожної з методик.

1.2.1 Метод STRIDE

STRIDE була розроблена Лорен Конфельдером та Праерітом Гаргом у 1999 році з метою визначення потенційних вразливостей та загроз для продуктів компаній. Методологія спрямована на забезпечення відповідності додатків вимогам безпеки щодо тріади CIA з конфіденційності, цілісності та доступності, окрім авторизації, автентифікації та безвідмовності.

Згідно методології STRIDE передбачено такі основні види загроз, які буде наведено в таблиці 1.1

Таблиця 1.1 – Перелік основних загроз моделі STRIDE

Загроза	Властивість	Визначення
Підміна особистості	Автентифікація	Видавання себе за іншу особу
Підміна	Цілісність	Зміна даних та коду
Відмова	Безвідмовність	Заперечення власних дій
Розкриття інформації	Конфіденційність	Розкриття інформації перед неавторизованими користувачами
Відмова в обслуговуванні	Доступність	Відмова або погіршення обслуговування
Зловживання привілеями	Авторизація	Підвищення повноважень через неправомірну авторизацію

STRIDE є найдавнішою методологією моделювання загроз і допомагає визначити методи їхнього усунення, до того ж, відносно простою у використанні, хоча і може становити значні витрати в часі [7].

1.2.2 Методологія TRIKE

TRIKE – це відкрита методологія аналізу загроз, що зосереджується на аудиторському процесі з точки зору управління ризиками та захисту. Цей підхід враховує реалізацію, загрози та моделі ризиків, забезпечуючи прийнятний рівень ризику для кожного активу для зацікавлених сторін.

Мета TRIKE полягає в забезпеченні прийнятного рівня ризику для всіх зацікавлених сторін, спілкуватися з ними щодо впливу ризиків та допомагати їм зрозуміти і зменшити ризики для організації. Це дозволяє користувачам

координувати та співпрацювати завдяки вбудованій пріоритезації пом'якшення загроз та автоматизованим компонентам.

Використовуючи діаграми потоків даних, TRIKE створює ілюстрації потоків даних, що дозволяє користувачам виконувати дії в системі. Методологія дозволяє визначати та присвоювати значення ризику, а також створювати заходи безпеки для вирішення загроз. Проте великі системи можуть стикатися з труднощами при застосуванні цієї методології через необхідність розуміння всієї системи [8].

1.2.3 Метод OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) — методологія для оцінки організаційних ризиків, таких як вплив витоку даних на операційну діяльність компанії. Розроблена Університетом Карнегі-Меллона (США) та CERT Інституту програмної інженерії (SEI) у 2003 році, вона орієнтована на малі та середні підприємства до 100 осіб.

OCTAVE використовує підхід самостійного управління, де співробітники, зазвичай керівництво та операційні команди, визначають стратегію безпеки, що ускладнює масштабування, тому методологія підходить для невеликих організацій. Вона допомагає виявляти методи зниження ризиків, підвищує обізнаність щодо управління ризиками та сприяє командній співпраці. OCTAVE зменшує потребу в документації, є висококонфігурованою та забезпечує надійний огляд діяльності і послідовні результати [9].

1.2.4 Метод PASTA

Процес симуляції атак і аналізу загроз (PASTA) – це орієнтована на ризики методологія моделювання загроз, розроблена генеральним директором VerSprite Тоні Уседа-Велезом та лідером з безпеки Марко М. Мораном. PASTA має перевагу масштабованості, що робить її ідеальною для зростаючих бізнесів

та може залучати технічні команди та ключових осіб, що приймають рішення, забезпечуючи дотримання вимог відповідності та регуляторних потреб, а також врахування технічного обсягу та потенційних вразливостей.

PASTA дозволяє контекстуальний підхід, при якому технічні дії завжди пов’язані з бізнес-цілями та забезпечує моделювання загроз на основі доказів, підтримуючи мотиви загроз та використовуючи дані,

Згідно методології розробки моделі загроз PASTA пропонується 7-кроковий процес аналізу ризиків, що складається з таких дій:

- визначення цілей;
- визначення технічного обсягу;
- декомпозиція застосунку;
- аналіз загроз;
- аналіз вразливостей і слабких місць;
- моделювання атак;
- аналіз ризиків і впливу [10].

1.2.5 Метод VAST

Visual, Agile, Simple Threat Modeling (VAST) – це методологія моделювання загроз, розроблена творцями продукту ThreatModeler. Її мета – усунення прогалин у масштабованості підприємства шляхом інтеграції у весь життєвий цикл розробки програмного забезпечення (SDLC). VAST включає три основні складові, які підтримують масштабоване рішення для моделювання загроз.

Так, автоматизація відповідає за уникнення однакових завдань моделювання загроз та безперервність власне процесу моделювання загроз і завдяки масштабуванню охоплює усе підприємство.

Інтеграцією передбачено злагоджену роботу з інструментами протягом усього життєвого циклу ПЗ, окрім цього це – підтримка гнучкості технологій DevOps.

Співпраця передбачає роботу з ключовими стейкхолдерами, наприклад, розробниками додатків, системними архітекторами, командою з безпеки та старшими керівниками [11].

2.2Критерії оцінки захищеності комп'ютерних мереж

НД ТЗІ 2.5-004-99 або Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу (надалі – НСД) встановлює критерії оцінювання рівня захищеності комп’ютерних мереж від НСД. На їх основі визначаються вимоги до захищених комп’ютерних систем (надалі – КС), створюються захищені КС та засоби захисту від НСД.

Критерії надають:

- шкалу порівняння для оцінювання надійності захисних механізмів від НСД, розроблених в КС;

- основу для створення КС, де повинні бути реалізовані засоби захисту інформації.

Функціональні критерії поділяються на чотири категорії, кожна з яких описує вимоги до відповідних їм послуг для реалізації захисту від загроз в кожній з цих категорій, а саме критерії конфіденційності, цілісності, доступності, спостережності.

Крім функціональних критеріїв, існують також критерії гарантій, що дозволяють оцінити коректність реалізації послуг.

В цьому підрозділі наведено короткі теоретичні відомості про кожну з цих категорій критеріїв оцінки захищеності інформаційних систем [12, с. 10];

1.3.1 Критерії конфіденційності

Критерії конфіденційності розглядають загрози, пов’язані з несанкціонованим ознайомленням з інформацією.

Згідно цього розділу передбачено такі послуги: довірча конфіденційність (КД), адміністративна конфіденційність (КА), повторне використання об’єктів (КО), аналіз прихованих каналів (КК) та конфіденційність при обміні (КВ).

Короткий виклад кожної з послуг Критеріїв конфіденційності:

А) Довірча конфіденційність надає можливість користувачу керувати інформаційними потоками, що йдуть від захищених об’єктів, що належать його домену, до інших користувачів. Рівні даної послуги варіюються на підставі повноти захисту та вибірковості керування [12, с. 11];

Б) Адміністративна конфіденційність (КА) надає можливість адміністраторам або уповноваженим користувачам керувати потоками інформації від об’єктів до користувачів. Аналогідно до КД рівні даної послуги варіюються на підставі повноти захисту та вибірковості керування [12, с. 12];

В) Повторне використання об’єктів (КО) передбачає забезпечення правильного повторного використання розділюваних об’єктів з гарантіями відсутності інформації, що залишається після користувача або процеса, якщо один з них (ред. – об'єктів) надається наступному конкретному користувачу або процесу [12, с. 13];

Г) Аналіз прихованих каналів (КК) виконується з метою виявлення та усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги формуються на основі того, чи виконуються лише виявлення, контроль та перекриття прихованих каналів [12, с. 14];

Д) Конфіденційність при обміні (КВ) полягає в забезпеченні захисту об’єктів від НСД до інформації, що міститься в цих об’єктах, в процесі імпорту через незахищені канали [12, с. 15].

1.3.2 Критерії цілісності

Критерії цілісності розглядають загрози, пов’язані з несанкціонованою модифікацією інформації (зміна, знищення). Для оцінки КС на відповідність

вимогам цілісності, повинні надаватися послуги з захисту оброблюваної інформації від несанкціонованого внесення змін.

Згідно цього розділу передбачено такі послуги, зокрема, довірча цілісність (ЦД), адміністративна цілісність (ЦА), відкат (ЦО) та цілісність при обміні (КВ).

Короткий виклад кожної з послуг Критеріїв цілісності:

А) Довірча цілісність (ЦД) надає можливість користувачу керувати потоками інформації від інших користувачів до захищених об’єктів. Рівні вимог до цієї послуги формуються на основі оцінювання повноти захисту та вибіркового керування [12, с. 16];

Б) Адміністративна цілісність (ЦА) надає змогу адміністраторам та/або уповноваженим користувачам керувати потоками інформації від користувачів до захищених об’єктів. Як і у випадку з ЦД, рівні вимог до ЦА формуються на основі оцінки повноти захисту та вибіркового керування [12, с. 17];

В) Згідно послуги відкату (ЦО) передбачено можливість скасувати операцію / їх послідовність і повернення (відкат) захищеного об’єкта до попереднього стану. Рівні вимог до ЦО формуються на основі множини операцій, для яких наявна можливість здійснення відкату до попереднього стану [12, с. 18];

Г) Згідно послуги цілісності під час обміну (ЦВ) передбачено можливість захисту об’єктів від несанкціонованої зміни інформації при їхньому імпорті/експорті через незахищене середовище. [12, с. 19].

1.3.3 Критерії доступності

До критеріїв доступності слід віднести вимоги до забезпечення захисту від порушень можливості використання КС або оброблюваної інформації. Для оцінювання відповідності КС критеріям доступності, повинні надаватися

послуги щодо забезпечення загальної функціональності КС, окремих функцій або оброблюваної в певний час інформації та гарантувати відмовостійкість КС.

Забезпечення конфіденційності передбачено завдяки таким послугам як використання ресурсів (ДР), стійкість до відмов (ДС), гаряча заміна (ДЗ) та відновлення після збоїв (ДВ).

Короткий виклад кожної з послуг Критеріїв доступності:

А) Використання ресурсів (ДР) передбачає можливість користувачів керувати використанням послуг та ресурсів. Рівні цієї послуги засновані на підставі повноти захисту та вибірковості керування доступністю послуг КС [12, с. 20];

Б) Відмовостійкість (ДС) гарантує можливості використання інформації, окремих функцій або КС загалом навіть у разі відмови її компонента. Рівні її послуг побудовані на підставі можливості КЗЗ забезпечувати працездатність КС в залежності від кількості відмов та послуг, що залишилися доступними навіть після відмови [12, с. 21];

В) Гаряча заміна (ДЗ) полягає в гарантіях доступності КС (використання інформації, окремих функцій та КС загалом) в процесі заміни окремих компонентів. Рівні цієї послуги побудовані на підставі повноти реалізації заміни компонентів КС [12, с. 22];

Г) Відновлення після збоїв (ДВ) передбачає собою повернення до відомого захищеного стану після відмови та/або перебоїв в наданні послуг. Рівні вимог до даної послуги грунтуються на основі ступеня автоматизованості відновлювальних процесів [12, с. 23].

1.3.4 Критерії спостереженості

Для можливості оцінювання КС на предмет відповідності критеріям спостереженості, КЗЗ повинен гарантувати відповідальність користувачів за свої дії та гарантувати підтримку спроможності виконувати свої функції.

Забезпечення спостереженості КС гарантується переліком з таких послуг як реєстрація або аудит (НР), ідентифікація та автентифікація (НИ), достовірний канал (НК), розподіл обов'язків (НО), цілісність комплексу засобів захисту (НЦ), самотестування (НТ), ідентифікація та автентифікація при обміні (НВ), автентифікація відправника (НА) та автентифікація отримувача (НП).

Короткий виклад кожного з Критеріїв спостереженості:

А) Реєстрацією (НР) передбачено можливість контролювання небезпечних для КС дій. Рівні цієї послуги грунтуються на повноті та вибірковості контролю, складності засобів аналізу даних журналів реєстрації, а також спроможності виявити потенційні порушення [12, с. 24];

Б) Ідентифікацією та автентифікацією (НИ) передбачено можливість КЗЗ визначати та перевіряти особистість користувачів, що намагаються отримати доступ до КС. Рівні цієї послуги визначаються кількістю задіяних механізмів автентифікації [12, с. 25];

В) Згідно послуги достовірного каналу (НК) гарантується можливість користувача безпосередньо взаємодіяти з КЗЗ. Рівні даної послуги побудовані на наданні можливості КЗЗ або користувачу здійснювати захищений обмін [12, с. 26];

Г) Розподіл обов'язків (НО) дозволяє зменшити потенційні збитки від навмисних та ненавмисних (помилкових) дій користувачів та обмежити авторитарність керування. Рівні цієї послуги побудовані на підставі вибіркового керування можливостями користувачів та адміністраторів [12, с. 27];

Д) Цілісність комплексу засобів захисту (НЦ) передбачає визначення рівня можливості КЗЗ щодо самозахисту та керування захищеними об'єктами [12, с. 28];

Е) Самотестування (НТ) передбачає можливість КЗЗ перевіряти правильність функціонування та цілісність деяких функцій КС. Рівні цієї

послуги побудовані на можливості проведення тестування в процесі запуску або штатної роботи [12, с. 29];

Є) Згідно послуг ідентифікації та автентифікації при обміні (НВ) даними передбачена можливість одного КЗЗ ідентифікувати інший КЗЗ та навпаки, перш ніж почати взаємодію. Рівні цієї послуги побудовані на підставі повноти реалізації механізмів ідентифікації та автентифікації [12, с. 30];

Ж) Автентифікація відправника (НА) гарантує можливість захисту відмови від авторства і однозначне встановлення належності об'єкта його користувачу, тобто факт його створення та відправки. Рівні даної послуги базуються на основі можливості підтвердження результатів перевірки незалежною третьою стороною [12, с. 31];

З) Згідно автентифікації отримувача (НП) передбачено можливість захисту відмови від факту одержання об'єкта та встановити цей факт певним користувачем. Як і у випадку з НА, рівні даної послуги базуються на можливості підтвердження результатів перевірки третьою стороною [12, с. 32].

1.3.5 Критерії гарантій

Згідно Критеріїв гарантій передбачено такі вимоги, зокрема до архітектури КЗЗ, середовища та послідовності розробки, середовища функціонування, документації та випробувань КЗЗ. Передбачено сім ієрархічних рівнів гарантій. Вимоги укладаються у відповідності до розділів. Для отримання КС певного рівня гарантій (якщо не вищий) повинні бути задоволені всі вимоги до кожного з розділів.

Короткий виклад кожної з вимог до Критеріїв гарантій:

А) Архітектура – вимоги до архітектури гарантують, що КЗЗ спроможна повністю реалізувати політику безпеки [12, с. 33];

Б) Середовище розробки – вимоги до середовища розробки гарантують цілковиту керованість процесів розроблення та супроводження оцінюваної КС з боку Розробника [12, с. 34];

В) Послідовність розробки – вимоги до алгоритмів процесу проєктування гарантують наявність точного опису та відповідності реалізації КС вихідним вимогам (політиці безпеки) на кожній з стадій розробки [12, с. 35];

Г) Середовище функціонування – вимоги до функціонального середовища гарантують незмінність (відсутність несанкціонованого внесення змін) КС в процесі поставки Замовнику, а також інсталяції та ініціації Замовником у відповідності до вимог Розробника [12, с. 37];

Д) Документація – Розробник повинен надати опис послуг безпеки з боку КЗЗ та настанови адміністратору та користувачу щодо послуг безпеки. Окрім цього, повинні бути викладені основні принципи політики безпеки, а також самі послуги. Власне настанови повинні описувати властивості КС, засоби інсталяції, генерації та запуску КС, а також інструкції щодо використання адміністратором та користувачами послуг та функцій безпеки [12, с. 37];

Е) Випробування комплексу засобів захисту – передбачено наступні вимоги:

- подання Розробником для перевірки програми, процедури та методики випробувань усіх механізмів реалізації послуг безпеки;

- докази тестування у вигляді детального переліку результатів тестувань ;

- усунення уразливостей та повторне тестування КЗЗ для підтвердження відсутності недоліків та нових слабких місць;

- виконання тестів на подолання механізмів захисту та доведення факту відносної або абсолютної стійкості КЗЗ до атак з боку Розробника [12, с. 38].

1.4 Висновки до першого розділу

В першому розділі було описано політики безпеки, а саме дискреційну, мандатну та рольову, розглянуто коротко різні моделі побудови політик безпеки.

Згідно дискреційної політики безпеки передбачено розмежувальне керування доступом, однозначну ідентифікацію об’єктів і суб’єктів та визначення прав на основі певних зовнішніх правил. Мандатна політика гарантує доступ до інформації лише за умови наявності достатніх повноважень і не може переносити дані з вищого до нижчого рівня конфіденційності. Рольова політика безпека є самостійною та характеризується отриманням суб’єктами прав доступу на основі ролей.

Розглянуто короткі відомості та характеристики п’яти методологій побудови загроз, зокрема STRIDE, TRIKE, OCTAVE, PASTA та VAST. STRIDE орієнтована на забезпечення відповідності додатків вимогам безпеки тріади КЦД (конфіденційності, цілісності, доступності). TRIKE полягає в аудиті, співпраці, забезпеченні прийнятного рівня ризику і комунікації з зацікавленими сторонами щодо керування ризиками. OCTAVE використовує методи самостійного управління для визначення стратегії безпеки і орієнтована на невеликі підприємства. PASTA забезпечує контекстуальний підхід, грунтується на поєднанні заходів з бізнес-цілями, моделює загрози на основі доказів і мотивів загроз. VAST охоплює весь життєвий цикл ПЗ і полягає в усуненні прогалин в масштабованості підприємства, а також передбачає підтримку масштабованого моделювання.

Також проведено детальний аналіз кожної з складових Критеріїв оцінки захищеності інформаційних систем. Критерії оцінки в свою чергу поділяються на п’ять категорій, чотири з яких відносяться до Функціональних критеріїв безпеки (критерії конфіденційності, критерії цілісності, критерії доступності та критерії спостережності), а також і Критерії гарантій.

2 АНАЛІЗ ПОЛІТИК БЕЗПЕКИ, МОДЕЛЕЙ ЗАГРОЗ

2.1 Аналіз політик безпеки для захисту інформаційного ресурсу

Для чіткого розуміння, як вибудовувати політику безпеки, проаналізуємо усі вищезгадані моделі побудови політик безпеки (CIA, ZeroTrust, ISO 15408, ISO 27001), адже кожна з них має свої переваги та недоліки в залежності від інформаційних ресурсів, для яких вона розробляється і галузі свого практичного застосування.

2.2.6 Аналіз дискреційної політики безпеки

Серед переваг ДПБ можна згадати простоту реалізації відповідних захисних механізмів, завдяки чому саме положення ДПБ виконуються в більшості нині поширених захищених автоматизованих систем (надалі – АС).

Однак є і суттєві недоліки ДПБ:

- Незахищеність від шкідливих атак, що реалізуються програмами-троянами.
- Автоматичне визначення прав доступу суб’єкта до об’єкта без можливості задати їх вручну через постійну зміну в кількості об’єктів.
- Контроль поширення прав доступу: права на власність інформації можуть поширюватися при передаванні вмісту файлів.
- Питання визначення поширення доступу й аналіз впливу на АС: перед органом, що використовує ДПБ постає задача, яку неможливо вирішити алгоритмічно, а саме перевірка дій на наслідки для безпеки.

Таким чином, ДПБ і матриця доступу не є одним з кращих способів реалізації якісної і чіткої системи захисту інформації (надалі – СЗІ) [4, с. 104].

2.1.2 Аналіз мандатної політики безпеки

Мандатна політика безпеки характеризується рядом переваг, зокрема:

- Системи, побудовані на МПБ, характеризуються значно вищою надійністю завдяки контролю доступу не лише до об’єктів, а й стану АС. Канали витоку не є вбудованими і можуть виникнути на етапі практичної реалізації виключно через допущення розробником помилок;

- Простота та зрозумілість правил МПБ для розуміння тим, хто розробляє і користується АС, що також сприяє підвищенню рівня безпеки в системі.

- Здатність протистояти атакам з боку троянських конів.

- Можливість точно довести за допомогою математичних розрахунків підтримку системою політик безпеки.

Проте не обійшлося і без недоліків даного виду ПБ: практична реалізація МПБ є доволі складною і вимагає значних обчислювальних ресурсів, що можуть спричиняти навантаження на пристрої. Даний недолік пояснюється надвеликою кількістю інформаційних потоків, які не завжди можна ідентифікувати, що і ускладнює реалізацію МПБ на практиці [4, с. 105].

2.1.3 Аналіз рольової політики безпеки

Рольова політика безпеки безпосередньо не гарантує безпеки, хоча при цьому визначає характер обмежень, виконання яких і є критерієм безпеки в системі. РПБ характеризується наступними перевагами, зокрема:

- гнучкість;
- широкі можливості;
- простота та зрозумілість правил доступу;
- легке керування ролями в порівнянні з суб’єктами;
- можливість паралельного використання разом з іншими ПБ;
- можливість створення багаторівневих схем контролю доступу.

Проте є і недолік – хоча РПБ сприяє створенню простих, зрозумілих правил доступу, які легко застосувати на практиці, це також позбавляє АС теоретичної доказової бази.

Легкість в управлінні ролями пояснюється тим, що це значно більше підходить під поширені технології обробки інформації, якими передбачено розподіл обов'язків та галузей відповідальності між користувачами [4, с. 107].

2.1.4 Вибір моделі побудови політики безпеки

Дискреційна модель політики безпеки проста в реалізації і поширена в більшості АС, проте уразлива проти троянських програм, регулюється автоматично без можливості коригування її вручну і не вирішується алгоритмічно, таким чином, ДПБ не є найкращим методом, якщо планується побудова якісної та чітко вираженої системи захисту, тому вона не буде використана для розробки ПБ інформаційного ресурсу [4, с. 104].

Мандатна політика безпеки не лише захищена від атак з боку троянів, на відміну від ДПБ, а й має прості та зрозумілі правила для розробників та пересічних користувачів, надійніший контроль доступу, що застосовується не тільки до об'єктів, а й АС загалом, хоча й вимагає вищої потужності електронно-обчислювальних машин, особливо у випадку з розробкою ПБ для інформаційних порталів на зразок AllTransUA [4, с. 105].

Рольова політика безпеки характеризується гнучкістю, широкими можливостями налаштування прав доступу та їх керуванням, що забезпечується високим різноманіттям ролей в інформаційному ресурсі AllTransUA, що є доволі важливим через різні рівні можливостей користувачів. Також РПБ передбачає прості й зрозумілі правила доступу, які забезпечують ефективне керування ролями та правами доступу. Хоча теоретична доказова база для доведення безпеки і відсутня, практична реалізація РПБ забезпечує належний рівень контролю доступу і безпеки [4, с. 107].

Таким чином, для розробки політики безпеки сайту AllTransUA буде використана саме рольова модель безпеки.

2.2Аналіз моделей загроз

Для чіткого розуміння того, як створити модель загроз, проведемо аналітику кожної з методологій побудови моделі загроз, адже кожна з моделей має різні сфери застосування і власне переваги, недоліки та інші нюанси, які слід враховувати при розробці моделі загроз за тою чи іншою методологією.

2.2.1 Метод STRIDE

Серед переваг методики використання STRIDE можна виділити наступні властивості:

- Гнучкість: методологію можна використовувати в різних галузях.
- Вказання можливих помилок: допомагає у визначенні потенційних векторів атак, активів та техніки.
- Пріоритезація ризиків: допомагає командам визначати пріоритетні ризики та керувати ними, зосереджуючись на необхідних заходах безпеки.
- Зменшення кількості порушень: належне використання знижує ймовірність виникнення порушень безпеки.

Проте не варто забувати і про обмеження та недоліки, якими характеризується ця методологія:

- Ресурсоємність: аналітика загроз, векторів атак вимагає витрат не лише в часі, а й в ресурсах.
- Статичний аналіз: зосереджується на аналізі дизайну та архітектури, пропускаючи динамічні загрози.
- Суб'єктивність: оцінка загроз може бути суб'єктивною і відрізнятися між командами.

- Постійне обслуговування: потребує повторення для відображення змін у системі.

- Обмежена до програмного забезпечення: переважно призначена для моделювання загроз у розробці ПЗ.

Нюанси, які варто враховувати при моделюванні загроз за методологією STRIDE:

- Не скасовується необхідність в тестуванні безпеки: тест на проникнення та перевірка коду залишаються при цьому обов’язковими.

- Грунтується на експертності: вимагається наявність рівня знань та навичок у моделюванні загроз і безпеці.

- Нетехнічні загрози: загрози в галузі соціальної інженерії або фізичної безпеки можуть бути не врахованими [7].

2.2.6 Метод TRIKE

Серед переваг методології побудови моделі загроз за технологією TRIKE варто виділити наступні характеристики:

- Цілісний підхід: TRIKE враховує бізнес, додатки та технології, пропонуючи комплексний погляд на безпеку.

- Співпраця: сприяє координації та співпраці між зацікавленими сторонами.

- Пріоритезація: вбудована пріоритезація заходів з пом’якшення загроз і визначення запобіжних заходів.

- Управління ризиками: аналіз загроз з визначенням значення ризику, що допомагає в управлінні ризиками.

- Візуалізація: використання візуальних моделей для кращого розуміння сценаріїв загроз.

Серед недоліків даної методології слід виділити такі обмеження:

- Складність: потребує високого рівня експертності, що може бути викликом для менш досвідчених команд.
- Ресурсоємність: проведення аналізу займає багато часу і потребує навчання.
- Узгодження: важко узгодити заходи безпеки з бізнес-цілями, особливо при конкуруючих пріоритетах [8].

2.2.6 Метод OCTAVE

Серед переваг методу OCTAVE варто виділити наступні характеристики:

- Формує культуру безпеки: OCTAVE сприяє розвитку культури обізнаності щодо безпеки та проактивного управління ризиками в організації.
- Підвищує обізнаність у командах: Допомагає в управлінні ризиками та сприяє співпраці між командами.
- Економія часу: Зменшує потребу в надмірній документації та забезпечує повторювані та послідовні результати.
- Підтримує розробників: Надає надійний активоцентричний підхід і допомагає в ідентифікації методів пом'якшення.
- Самокерованість: OCTAVE високо налаштовується для команд безпеки та ризикових середовищ.

OCTAVE – це самокерований підхід, де відповідальність за встановлення стратегії безпеки бере на себе організація, що може ускладнити масштабування. Методологія також передбачає, що компанія має глибокі знання про бізнес та процеси безпеки і може самостійно виконувати всі необхідні дії.

Слід також пам’ятати, що OCTAVE має ряд певних обмежень, на які слід зважати при складанні моделі загроз:

- Складність інтеграції: інтеграція OCTAVE у існуючі процеси та робочі потоки організації може бути складною, особливо для добре встановлених практик.

- Охоплює не всі загрози: можливі нові або нетрадиційні загрози попри комплексний підхід OCTAVE.

- Великий обсяг документації: необхідність створення обширної документації, що може бути важким для управління, особливо в гнучких або швидкоплинних середовищах розробки [9].

2.2.4 Метод PASTA

Переваги використання PASTA полягають в співпраці, а саме можливості узгодити зусилля з безпеки з бізнес-цілями, налагоджувати співпрацю відділів та захищати важливі активи та процеси. Така методологія легко адаптовується під конкретні галузі і є гнучкою, аналізує вплив загроз на бізнес з урахуванням цілей та перспектив порушників. Окрім цього, PASTA використовує дані для обгрунтування мотивів загроз та концентрується на діях нападника з оцінкою імовірності та наслідків атаки на основі симуляції дійсних сценаріїв атак.

Методологія PASTA узгоджує бізнес-цілі та технічні вимоги, сприяє командній співпраці та залученню керівників. Завдяки орієнтації на ризики та багатоетапний процес, PASTA охоплює технічний обсяг, можливі вразливості та вимоги до відповідності і надає вивід, орієнтований на активи, з пріоритетним інвентарем та оцінкою.

Проте є і обмеження PASTA, які слід враховувати, перш ніж створювати модель загроз:

- Складність виконання: вимагає високого рівня експертності, що може бути викликом для менш досвідчених команд.

- Залежність від даних: ефективність залежить від якості наявних даних про систему.

- Масштабованість: великі або розподілені системи можуть створювати додаткові виклики для аналізу [10].

2.2.5 Метод VAST

Масштабоване моделювання загроз вимагає співпраці зацікавлених сторін, використовуючи їхні різноманітні навички та знання для оцінки загроз і визначення пріоритетів у зниженні ризиків. Без співпраці неможливо досягти загальноорганізаційного уявлення загроз. Натомість, спільна робота допомагає масштабувати моделювання загроз на всі етапи SDLC і краще реагувати на нові загрози, розуміючи ризики проекту в цілому.

Інтеграція з Agile та іншими виробничими інструментами створює основу для спільного процесу моделювання загроз. Використання VAST забезпечує цілісне уявлення всієї поверхні атаки, дозволяючи проекту мінімізувати загальний ризик.

Власне методологія VAST має такі переваги:

- Масштабованість: VAST дозволяє ефективно масштабувати моделювання загроз, охоплюючи всі етапи SDLC (Software Development Life Cycle);

- Інтеграція з Agile: легко інтегрується з Agile-методологіями, що сприяє швидкому реагуванню на нові загрози;

- Співпраця: сприяє активній співпраці між зацікавленими сторонами, використовуючи їхні різноманітні навички та знання для оцінки загроз і зниження ризиків;

- Цілісне уявлення загроз: забезпечує комплексний огляд всієї поверхні атаки, що дозволяє мінімізувати загальний ризик для проекту;

- Простота використання: проста у використанні методологія, яка дозволяє швидко зрозуміти та застосувати процеси моделювання загроз;

- Ефективність у зниженні ризиків: допомагає визначати пріоритети у зниженні рівня ризиків, забезпечуючи глибше розуміння ризиків, пов'язаних з проектом.

Недоліки методології побудови моделей загроз VAST:

- Вимоги до співпраці: вимагає активної співпраці між всіма зацікавленими сторонами, що може бути складним у великих або розподілених командах;

- Інтеграційні виклики: може виникати складність при інтеграції з існуючими інструментами та процесами організації, особливо в умовах традиційного або менш гнучкого робочого середовища;

- Навчання та адаптація: потребує часу на навчання та адаптацію команди до нової методології, що може затримати впровадження процесу моделювання загроз;

- Залежність від якості даних: ефективність методології залежить від якості та точності наявних даних про систему та її архітектуру.

Ці переваги та недоліки дозволяють оцінити, чи підходить методологія VAST для конкретних потреб і умов організації та інформаційно-комунікаційної системи [11].

2.2.6 Вибір методології побудови моделі загроз

Хоча методика TRIKE передбачає співпрацю між зацікавленими сторонами та пріоретизує заходи з пом’якшення наслідків загроз, візуальну демонстрацію сценаріїв загроз, вона також передбачає роботу з бізнесом, що однозначно не поєднується з ціллю інформаційного ресурсу, який розроблений передусім з пізнавальною метою. Тому TRIKE не є найкращою методикою побудови моделі загроз для некомерційних ресурсів на зразок AllTransUA.

OCTAVE зосереджується на організаційному рівні ризик-менеджменту, включаючи в себе оцінку активів, загроз та вразливостей з точки зору бізнесу та управління, що робить методологію складною та ресурсозатратною. Окрім цього, цією методологією передбачено детальний багатоетапний затратний процес і вона підходить лише для невеликих організацій. Власне з цих причин OCTAVE не може вважатися оптимальним вибором для некомерційного ресурсу AllTransUA.

Методика PASTA підходить, якщо потрібно розробити модель загроз для бізнес-підприємств аналогічно до TRIKE і також вимагає високого рівня обізнаності, опирається на якість даних про систему та масштабованість систем, що ускладнює аналіз для менш досвідчених працівників. Тому PASTA також не є найкращим рішенням у побудові моделі загроз.

Методологія VAST підходить для життєвого циклу розробки програмного забезпечення SDLC. Оскільки модель загроз будується для уже існуючого інформаційного ресурсу AllTransUA, який постійно оновлюється, охопити всі цикли SDLC буде непосильною задачею, що є причиною невідповідності VAST поставленому завданню.

3.2 Висновки до другого розділу

В другому розділі було розглянуто всі особливості, переваги та недоліки політик безпеки, зокрема дискреційної, мандатної та рольової моделей безпеки, а також методологій побудови моделі загроз.

Рольова політика безпеки характеризується гнучкістю, широкими можливостями налаштування прав доступу та їх керуванням, що забезпечується високим різноманіттям ролей в інформаційному ресурсі AllTransUA, що є доволі важливим через різні рівні можливостей користувачів. Також РПБ передбачає прості й зрозумілі правила доступу, які забезпечують ефективне керування ролями та правами доступу. Хоча теоретична доказова

база для доведення безпеки і відсутня, практична реалізація РПБ забезпечує належний рівень контролю доступу і безпеки.

Серед методологій побудови моделі загроз було розглянуто такі методики як STRIDE, TRIKE, OCTAVE, PASTA та VAST.

Оскільки підхід STRIDE є доволі гнучким і може застосовуватися в різних галузях, включно і в галузі доопрацювання безпеки інформаційних ресурсів на прикладі сайту AllTransUA, зосереджується на аналізі дизайну та архітектури (що є доцільним у випадку добре продуманого дизайн-коду сайту), також оскільки інформаційний ресурс регулярно оновлюється, то перевірка коду та дизайну залишаються обов’язковими.

Таким чином, для розробки політики безпеки та моделі загроз було обрано рольову політику безпеки та методологію STRIDE.

3 ФОРМУВАННЯ МОДЕЛІ БЕЗПЕКИ НА ОСНОВІ ВИБРАНИХ МЕТОДОЛОГІЙ

3.1 Створення моделі загроз та порушника за вибраною методологією

Для розробки моделі загроз було обрано методологію STRIDE, адже вона характеризується гнучкістю і зосереджується на аналізі дизайну та архітектури, що має сенс у випадку продуманого дизайну сайту, а також обов'язковістю перевірок коду та дизайну (ресурс AllTransUA час від часу зазнає оновлень).

Для кожного з 6 компонентів методології STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial Of Service, Elevation Of Privileges) буде розроблено таблицю загроз з урахуванням походження порушників (зовнішні або внутрішні), властивості, на яку спрямована загроза, характер загрози (навмисні та ненавмисні), об'єкт впливу, середовище, ідентифікаційний номер загрози, детальний опис суті загрози, активи, що знаходяться під впливом цієї загрози.

3.1.1 Підміна особистості (Spoofing)

Оформлення моделі загроз типу Spoofing передбачає загрози, що спрямовані на підміну особистості з використанням різних технологій. В даному випадку маються на увазі способи отримання НСД до облікового запису користувачів і здійснення від їхнього імені різних правомірних дій з ціллю суто підставити інших користувачів. Таблицю методології загроз типу Spoofing представлено на рисунку 3.1:

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
S-001	Підміна особистості шляхом злому облікового запису простого користувача або користувачів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника та здійснення правомірних дій від його імені	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача	Втрата конфіденційності та цілісності даних
S-002	Підміна особистості шляхом злому облікового запису користувача/користувачів (включно і адміністраторів, модераторів та редакторів)	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів та здійснення дій від його імені з боку іншого користувача та здійснення правомірних дій від його імені	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача	Втрата конфіденційності та цілісності даних

Рисунок 3.1 – Таблиця загроз типу Spoofing

3.1.2 Зміна даних (Tampering)

Оформлення моделі загроз типу Tampering передбачає загрози, що спрямовані на зміну даних/коду з використанням різних технологій. В даному випадку маються на увазі способи отримання НСД до облікового запису користувачів і здійснення від їхнього імені змін параметрів облікового запису, неправомірних дій, що призводять до блокування облікових записів користувачів. Таблицю методології загроз типу Tampering представлено на рисунку 3.2 та рисунку 3.3 у вигляді двох частин.

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
T-001	Зламування облікового запису користувача/користувачів та знищення облікового запису/записів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку іншого користувача і здійснення неправомірних дій, що в результаті приводять до блокування облікового запису	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача	Втрата конфіденційності, цілісності та доступності
T-002	Зламування облікового запису користувача/користувачів та знищення облікового запису/записів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і здійснення неправомірних дій, що в результаті приводять до блокування облікового запису	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача	Втрата конфіденційності, цілісності та доступності
T-003	Зламування облікового запису користувача/користувачів та зміна атрибутів доступу до облікового запису користувача/користувачів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і зміни атрибутів доступу, що унеможливить доступ зламаним користувачам до облікових записів	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу користувача	Втрата конфіденційності, цілісності та доступності
T-004	Зламування облікового запису користувача/користувачів та зміна атрибутів доступу до облікового запису користувача/користувачів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і зміни атрибутів доступу, що унеможливить доступ зламаним користувачам до облікових записів	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу користувача	Втрата конфіденційності, цілісності та доступності

Рисунок 3.2 – Таблиця загроз типу Tampering (перша частина)

T-005	Підміна особистості шляхом злому облікового запису користувача/користувачів та знищення облікового запису/записів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку іншого користувача і здійснення неправомірних дій, що в результаті приводять до блокування облікового запису	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача	Втрата конфіденційності, цілісності та доступності
T-006	Зламування облікового запису користувача/користувачів та знищення облікового запису/записів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і здійснення неправомірних дій, що в результаті приводять до блокування облікового запису	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача	Втрата конфіденційності, цілісності та доступності
T-007	Зламування облікового запису користувача/користувачів та зміна атрибутів доступу до облікового запису користувача/користувачів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і зміни атрибутів доступу, що унеможливить доступ зламаним користувачам до облікових записів	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу користувача	Втрата конфіденційності, цілісності та доступності
T-008	Зламування облікового запису користувача/користувачів та зміна атрибутів доступу до облікового запису користувача/користувачів	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і зміни атрибутів доступу, що унеможливить доступ зламаним користувачам до облікових записів	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу користувача	Втрата конфіденційності, цілісності та доступності

Рисунок 3.3 – Таблиця загроз типу Tampering (друга частина)

3.1.3 Відмова від авторства (Repudiation)

Оформлення моделі загроз типу Repudiation передбачає загрози, що стосуються заперечення власних дій порушником. В даному випадку маються на увазі способи заперечення власних дій у вигляді використання засобів шифрування зв’язку та використання чужої IP-адреси при здійсненні НСД. Таблицю методології загроз типу Repudiation представлено на рисунку 3.4 та рисунку 3.5 у вигляді двох частин.

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
R-001	Зламування облікового запису користувача/користувачів з використанням засобів шифрування з'єднання	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку іншого користувача з використанням засобів шифрування зв'язку (VPN) та маскуванням під адресу третього з користувачів	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача	Втрата конфіденційності та цілісності даних
R-002	Зламування облікового запису користувача/користувачів з використанням засобів шифрування з'єднання	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника з використанням засобів шифрування зв'язку (VPN) та маскуванням під адресу третього з користувачів	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача	Втрата конфіденційності та цілісності даних
R-003	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду під свої потреби з використанням засобів шифрування з'єднання	Загроза полягає в отриманні НСД до облікового запису адміністраторів з боку зовнішнього порушника, зміни атрибутів доступу та функціональності коду під свої потреби з використанням засобів шифрування зв'язку (VPN) та маскуванням під адресу третього з користувачів	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних

Рисунок 3.4 – Таблиця загроз типу Repudiation (частина 1)

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
R-004	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду під свої потреби з використанням засобів шифрування з'єднання	Загроза полягає в отриманні НСД до облікового запису адміністраторів з боку іншого користувача, зміни атрибутів доступу та функціональності коду під свої потреби з використанням засобів шифрування зв'язку (VPN) та маскуванням під адресу третього з користувачів	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних
R-005	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду з ціллю погіршення функціональності сайту з використанням засобів шифрування з'єднання	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку іншого користувача, зміни атрибутів доступу адміністратора та функціональності коду сайту з ціллю погіршення його функціонування з використанням засобів шифрування зв'язку (VPN) та маскуванням під адресу третього з користувачів	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних
R-006	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду з ціллю погіршення функціональності сайту з використанням засобів шифрування з'єднання	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника, зміни атрибутів доступу адміністратора та функціональності коду сайту з ціллю погіршення його функціонування з використанням засобів шифрування зв'язку (VPN) та маскуванням під адресу третього з користувачів	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних

Рисунок 3.5 – Таблиця загроз типу Repudiation (частина 2)

3.1.4 Розкриття інформації (Information Disclosure)

Оформлення моделі загроз типу Information Disclosure передбачає загрози, що спрямовані на розкриття небажаної для поширення інформації, до прикладу, програмного коду, відомих уразливостей та недоліків сайту AllTransUA або навіть ненавмисні загрози, коли користувачі та адміністратори з власної необережності розкривають свої дані та атрибути доступу, а також програмний код та вразливості, які можуть бути використані для реалізації загроз типу Denial Of Service. Таблицю методології загроз типу Information Disclosure представлено на рисунку 3.6 та рисунку 3.7 у вигляді двох частин.

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
I-001	Зламування облікового запису користувача/користувачів і публікація атрибутів доступу	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку іншого користувача і публікації атрибутів доступу в межах сайту (дописи, форуми для обговорення, коментарі)	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу користувача	Втрата конфіденційності
I-002	Зламування облікового запису користувача/користувачів і публікація атрибутів доступу	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і публікації атрибутів доступу в межах сайту (дописи, форуми для обговорення, коментарі)	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу користувача	Втрата конфіденційності
I-003	Зламування облікового запису адміністратора та публікація їхніх атрибутів доступу	Загроза полягає в отриманні НСД до облікового запису адміністратора з боку зовнішнього порушника і публікації атрибутів доступу адміністратора в межах сайту (дописи, форуми для обговорення, коментарі) та наданні можливості іншим користувачам проваджувати діяльність від імені адміністратора	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу адміністратора	Втрата конфіденційності та цілісності даних
I-004	Зламування облікового запису адміністратора та публікація їхніх атрибутів доступу	Загроза полягає в отриманні НСД до облікового запису адміністратора з боку користувача і публікації атрибутів доступу адміністратора в межах сайту (дописи, форуми для обговорення, коментарі) та наданні можливості іншим користувачам проваджувати діяльність від імені адміністратора	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу адміністратора	Втрата конфіденційності та цілісності даних

Рисунок 3.6 – Таблиця загроз типу Information Disclosure (частина 1)

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
I-005	Зламування облікового запису адміністратора та оприлюднення уразливостей та програмного коду	Загроза полягає в отриманні НСД до облікового запису адміністратора з боку користувача і публікації уразливості (наприклад, уразливого програмного коду) з ціллю надання можливості користувачам використати ці вразливості в різних цілях та організовувати атаки на сайт	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних
I-006	Зламування облікового запису адміністратора та оприлюднення уразливостей та програмного коду	Загроза полягає в отриманні НСД до облікового запису адміністратора з боку зовнішнього порушника і публікації уразливості (наприклад, уразливого програмного коду) з ціллю надання можливості користувачам використати ці вразливості в різних цілях та організовувати атаки на сайт	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних
I-007	Публікація користувачем даних про свій обліковий запис та атрибути доступу	Загроза полягає в ненавмисній публікації користувачем в коментарях до фото/дописів/обговорень своїх облікових даних	Логічне	Внутрішній порушник	Ненавмисно	Обліковий запис та атрибути доступу користувача.	Втрата конфіденційності
I-008	Публікація адміністратором даних про свій обліковий запис, атрибути доступу, уразливості та програмний код	Загроза полягає в ненавмисній публікації адміністратором в коментарях до фото/дописів/обговорень своїх облікових даних, програмного коду	Логічне	Внутрішній порушник	Ненавмисно	Програмний код, обліковий запис та атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності

Рисунок 3.7 – Таблиця загроз типу Information Disclosure (частина 2)

3.1.5 Відмова в обслуговуванні (Denial Of Service)

Оформлення моделі загроз типу Denial Of Service передбачає загрози, що спрямовані на зміну даних/коду з використанням різних технологій, зокрема під свої потреби або з ціллю погіршення функціональності сайту. В даному випадку маються на увазі способи отримання НСД до облікового запису користувачів та подальше здійснення від їхнього імені змін параметрів облікового запису, неправомірних дій, що призводять до блокування облікових записів користувачів, тобто також мають місце й загрози типу Tampering. Таблицю методології загроз типу Denial Of Service представлено на рисунку 3.8, рисунку 3.9 та рисунку 3.10 у вигляді трьох частин.

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
D-001	Зламування облікового запису адміністраторів та зміна програмного коду під свої потреби	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і зміни функціональності коду під свої потреби	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, засоби для функціонування сайту	Втрата конфіденційності та цілісності даних
D-002	Зламування облікового запису адміністраторів та зміна програмного коду під свої потреби	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку користувача сайту і зміни функціональності коду під свої потреби	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу користувача	Втрата конфіденційності та цілісності даних
D-003	Зламування облікового запису адміністраторів та зміна програмного коду з ціллю погіршення функціональності сайту	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника і зміни функціональності коду сайту з ціллю погіршення його функціонування	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних
D-004	Зламування облікового запису адміністраторів та зміна програмного коду з ціллю погіршення функціональності сайту	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку іншого користувача і зміни функціональності коду сайту з ціллю погіршення його функціонування	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних

Рисунок 3.8 – Таблиця загроз типу Denial Of Service (частина 1)

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
D-005	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду з ціллю погіршення функціональності сайту	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку іншого користувача, зміни атрибутів доступу адміністратора та функціональності коду сайту з ціллю погіршення його функціонування	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних
D-006	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду з ціллю погіршення функціональності сайту	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника, зміни атрибутів доступу адміністратора та функціональності коду сайту з ціллю погіршення його функціонування	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних
D-007	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду під свої потреби	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку зовнішнього порушника, зміни атрибутів доступу та функціональності коду під свої потреби	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних
D-008	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду під свої потреби	Загроза полягає в отриманні НСД до облікового запису користувача/користувачів з боку іншого користувача сайту, зміни атрибутів доступу та функціональності коду під свої потреби	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис користувача, атрибути доступу адміністратора, засоби для функціонування сайту	Втрата конфіденційності, цілісності та доступності даних

Рисунок 3.9 – Таблиця загроз типу Denial Of Service (частина 2)

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
D-009	Здійснення DOS/DDOS атак на сайт	Загроза полягає в здійсненні DOS/DDOS атак на сайт з боку зовнішнього порушника з метою виведення функціональності сайту з ладу	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, засоби для функціонування сайту	Втрата цілісності та доступності даних
D-010	Зламування облікового запису адміністраторів, зміна їхніх атрибутів доступу та зміна програмного коду під свої потреби	Загроза полягає в здійсненні DOS/DDOS атак на сайт з боку користувача з метою виведення функціональності сайту з ладу	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, засоби для функціонування сайту	Втрата цілісності та доступності даних
D-011	Здійснення DOS/DDOS атак на сайт з використанням засобів шифрування з'єднання	Загроза полягає в здійсненні DOS/DDOS атак на сайт з боку зовнішнього порушника з метою виведення функціональності сайту з ладу з використанням засобів шифрування зв'язку (VPN) з ціллю маскування під третього користувача	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, засоби для функціонування сайту	Втрата цілісності та доступності даних
D-012	Здійснення DOS/DDOS атак на сайт з використанням засобів шифрування з'єднання	Загроза полягає в здійсненні DOS/DDOS атак на сайт з боку користувача з метою виведення функціональності сайту з ладу з використанням засобів шифрування зв'язку (VPN) з ціллю маскування під третього користувача	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, засоби для функціонування сайту	Втрата цілісності та доступності даних

Рисунок 3.10 – Таблиця загроз типу Denial Of Service (частина 3)

3.1.6 Незаконне підвищення привілеїв (Elevation Of Privileges)

Оформлення моделі загроз типу Elevation Of Privileges передбачає загрози, що спрямовані на отримання НСД до вищих посад на сайті (локального та загального редактора, модератора коментарів та фотографій та адміністратора). В даному випадку маються на увазі способи отримання НСД до облікового запису користувачів з найвищими привілеями і здійснення від їхнього імені надання вищих посад пересічним користувачам. Таблицю методології загроз типу Elevation Of Privileges представлено на рисунку 3.11.

ID загрози	Категорія загрози	Опис загрози	Середовище	Джерело	Характер виконання	Активи	Наслідки реалізації
E-001	Зламування облікового запису адміністраторів та роздавання привілеїв іншим користувачам	Загроза полягає в отриманні НСД до облікового запису адміністраторів з боку користувача та підвищення повноважень іншому користувачу/користувачам	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу адміністратора	Втрата конфіденційності
E-002	Зламування облікового запису адміністраторів та роздавання привілеїв іншим користувачам	Загроза полягає в отриманні НСД до облікового запису адміністраторів з боку зовнішнього порушника та підвищення повноважень іншому користувачу/користувачам	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу адміністратора	Втрата конфіденційності
E-003	Зламування облікового запису адміністраторів та роздавання привілеїв іншим користувачам з використанням засобів шифрування з'єднання	Загроза полягає в отриманні НСД до облікового запису адміністраторів з боку зовнішнього порушника та підвищення повноважень іншому користувачу/користувачам з використанням засобів шифрування зв'язку (VPN) та маскуванням під адресу третього з користувачів	Логічне	Зовнішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу адміністратора	Втрата конфіденційності
E-004	Зламування облікового запису адміністраторів та роздавання привілеїв іншим користувачам з використанням засобів шифрування з'єднання	Загроза полягає в отриманні НСД до облікового запису адміністраторів з боку користувача та підвищення повноважень іншому користувачу/користувачам з використанням засобів шифрування зв'язку (VPN) та маскуванням під адресу третього з користувачів	Логічне	Внутрішній порушник	Навмисно	Апаратура, обладнання, програмне забезпечення, обліковий запис та атрибути доступу адміністратора	Втрата конфіденційності

Рисунок 3.11 – Таблиця загроз типу Elevation Of Privileges

Оскільки загрози більшості категорій (зокрема, загрози типів Spoofing, Tampering, Denial Of Service, Elevation Of Privileges) стосуються зламу акаунтів, рекомендується впровадити в сайт політику надійності паролів, яка успішно практикується на різних сайтах (складні паролі буде важче зламувати), а також впровадити багатофакторну автентифікацію, наприклад, перевірка по обличчю / паспорту. Це:

- забезпечить як і зміцнений захист (користувач отримає сповіщення на своєму пристрої про спроби отримання НСД і зможе вжити необхідних заходів, адже зловмиснику треба буде використати ще один засіб, аби підтвердити ”не свою” особистість);

- вбереже сайт від спроби створення обхідних версій заблокованого облікового запису через порушення правил завантаження контенту та поведінки на сайті з тої ж причини (користувачу, що порушив був правила завантаження контенту та поведінки на AllTransUA, доведеться використовувати ті ж біометричні дані, тобто перевірку по обличчю / паспорту);
- якщо користувач має два і більше облікових записи (до прикладу – один для творчих художніх фотографій, а другий – для наповнення бази), в разі порушення хоча б одним з них правил і як наслідок, блокування адміністраторами, автоматично блокуватиметься й інший обліковий запис цього користувача, адже вони є прив'язаними до одних і тих ж біометричних даних: результатів перевірки по обличчю / паспорту, що убезпечить сайт від підривної діяльності і зможе запобігти повторним атакам з боку однієї і тієї ж особи / групи осіб.

Вслід за цим, впровадження політики паролів та багатофакторна автентифікація допоможуть в зменшенні ризику здійснення більшості загроз з шести згаданих категорій, особливо типу Spoofing, Tampering та Denial Of Service, політика паролів забезпечить відсутність можливості створення паролів, які зламуються порівняно легко і швидко, а впровадження плагіну щодо переконання в правильності здійснюваних дій (діалогове вікно на зразок "Ви впевнені, що хочете опублікувати цей коментар?") убезпечить користувача від ненавмисної публікації небажаної інформації (наприклад, коли адміністратор/користувач може забути, що копіював цю інформацію і поспіхом натискає кнопку публікації коментаря).

3.2 Формування критеріїв оцінки захищеності інформаційного ресурсу

Сформуємо критерії, за якими буде проводитися оцінка захищеності інформаційно-пізнавального ресурсу AllTransUA. 47ротес першу ідентифікуємо, кого і що слід розуміти під наступними поняттями:

Об'єкти – фотографії, дописи, коментарі, облікові записи користувачів сайту AllTransUA, інформація про кількість переглядів, вподобайок та супер-вподобайок на фото.

Суб’єкти – зареєстровані користувачі (прості користувачі, локальні редактори, загальні редактори, модератори фотографій, модератори коментарів, адміністратори) та незареєстровані користувачі.

Захищені об’єкти – інформація про кількість переглядів, вподобайок та супер-вподобайок, облікові записи користувачів сайту AllTransUA.

3.2.1 Критерії конфіденційності

З урахуванням тематики та функціональності транспортного ресурсу AllTransUA маємо наступні вимоги щодо дотримання вимог конфіденційності:

А) Довірча конфіденційність (КД) повинна гарантувати користувачам можливість контролювання доступу до їхніх даних, а саме встановлювати конфіденційність відносно виставлених оцінок до фото та налаштовувати видимість особистої інформації;

Б) Адміністративна конфіденційність (КА) повинна гарантувати адміністраторам та модераторам можливість керувати доступом до інформації на сайті, а саме ухвалювати рішення щодо допуску або відхилення фотографій та коментарів для публікації, керувати ролями користувачів (підвищувати чи знижувати їхні привілеї);

В) Повторне використання об’єктів (КО) повинне гарантувати безповоротне остаточне видалення фотографій та коментарів користувача задля захищеності від надлишкової небажаної інформації, яка може зашкодити іншим користувачам;

Г) Згідно послуги аналізу прихованих каналів (КК) повинно здійснюватися виконання адміністраторами регулярної безпекової аналітики з ціллю виявлення прихованих каналів витоку інформації (наприклад, злиття в

публічний доступ осіб, що натиснули “подобається” / “дуже подобається” відносно фотографії/допису та перелік вподобаних особою фотографій/дописів, а також їхніх особистих даних, наявних в профілі), що може посягати на конфіденційність користувачів;

Д) Конфіденційність під час обміну (КВ) повинна гарантувати використання захищеного HTTPS-з’єднання для шифрування даних, що передаються між користувачами та сервером [12, с. 11-15].

Згідно результатів аналітики Критеріїв конфіденційності маємо наступні результати:

- КД досягається завдяки наявності функції модерування коментарів, проте виконується модерація коментарів лише в разі крайньої необхідності (якщо користувач систематично публікує неприйнятну інформацію і не дотримується етикету, він за рішенням адміністрації переходить в режим премодерації коментарів, а якщо має обліковий запис в чат-програмі Telegram, то детально буде повідомлений про перехід на модерацію). Також КД досягається можливістю перегляду інформації про користувача в профілі іншими користувачами та приховуванням інформації про те, хто переглядав та/або вподобав фотографію. Один з прикладів ДК показано на рисунку 3.12:

Рисунок 3.12 – Зразок дотримання КД на прикладі захисту інформації про осіб, що вподобали це фото

- КА досягається завдяки наявності можливості функції премодерації фотографій, яка відбувається лише пост-фактум (користувач переводиться в режим премодерації фотографій лише у разі систематичного публікування фотографій незадовільної якості, що можуть становити неприємності для інших користувачів сайту AllTransUA згідно рішення адміністрації, про зняття премодерації фото адміністрація повідомить додатково, до прикладу, через Telegram-чат), систему премодерації (рисунок 3.13), також КА досягається завдяки особливій політиці щодо неавторських фотографій (рисунки 3.14 та 3.15), до яких в будь-якому випадку застосовується премодерація задля дотримання ЗУ ”Про авторське право та суміжні права”;

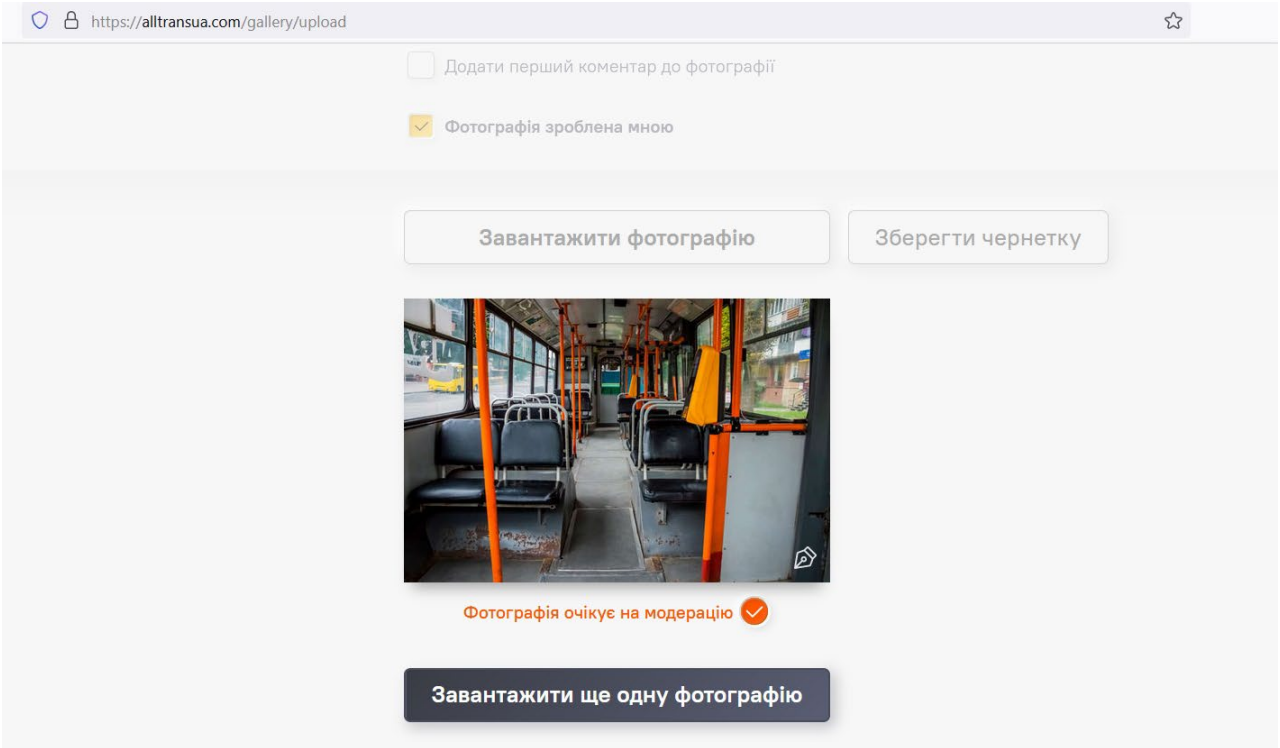

Рисунок 3.13 – Дотримання КА на прикладі модерації фотографій (набирає чинності лише після відповідного рішення адміністрації сайту)

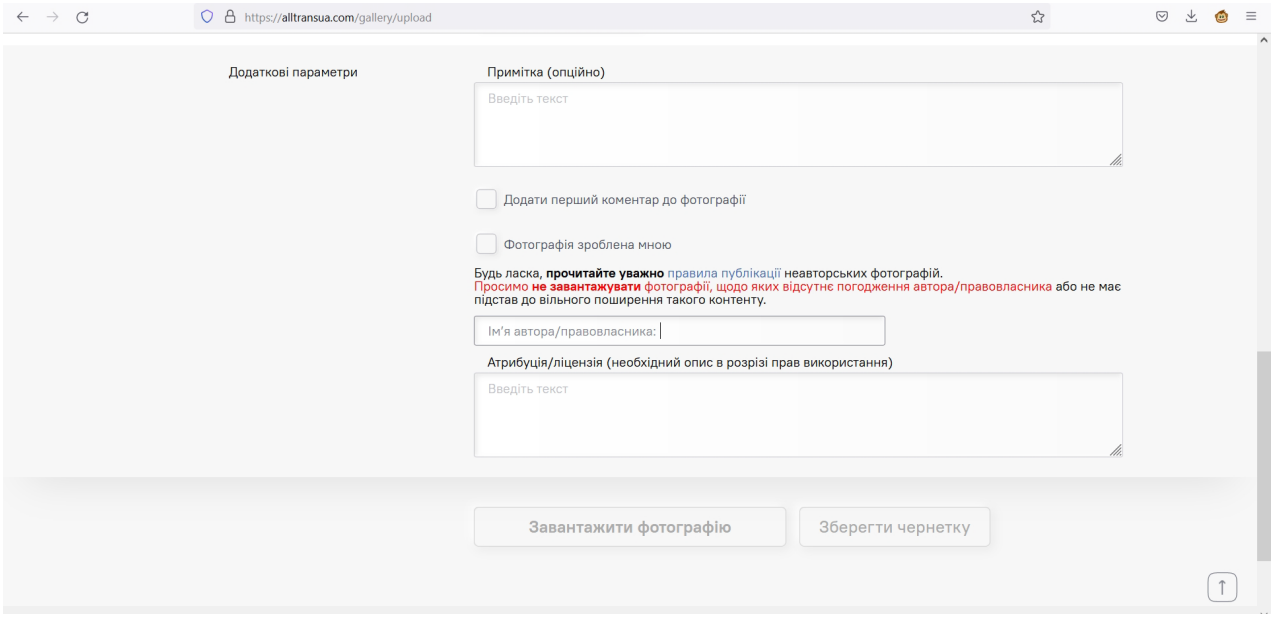

Рисунок 3.14 – Дотримання КА на прикладі особливої політики щодо неавторських фотографій

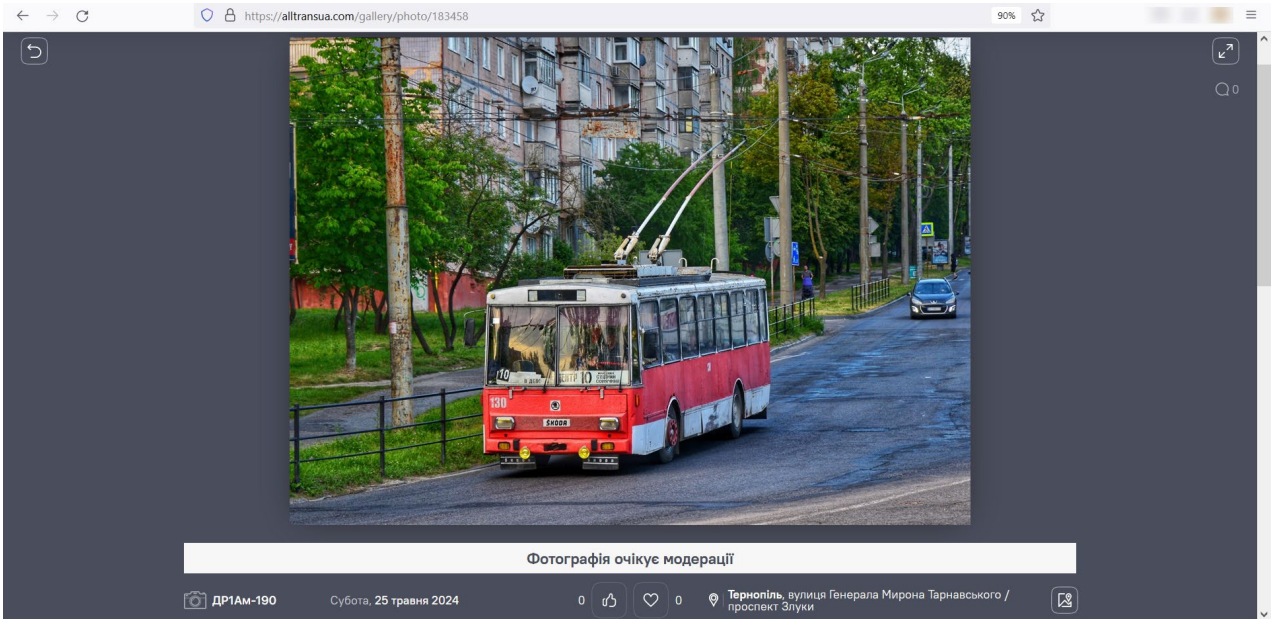

Рисунок 3.15 – Дотримання КА на прикладі особливої політики щодо неавторських фотографій

- КО досягається шляхом безповоротного видалення фотографій та коментарів у разі потреби, передбаченої адміністрацією сайту AllTransUA;
- В ході комунікації з адміністрацією сайту AllTransUA через канали зв'язку (наприклад, контакти адміністраторів в чат-програмі Telegram) було

з’ясовано, що регулярний аналіз безпеки на виявлення каналів витоку інформації не проводився, тому є проблема задоволення вимог КК;

- КВ досягається шляхом використання сайтом AllTransUA захищеного підключення HTTPS, що забезпечує безпеку даних при їхній передачі через незахищені канали, як видно на рисунку 3.16:

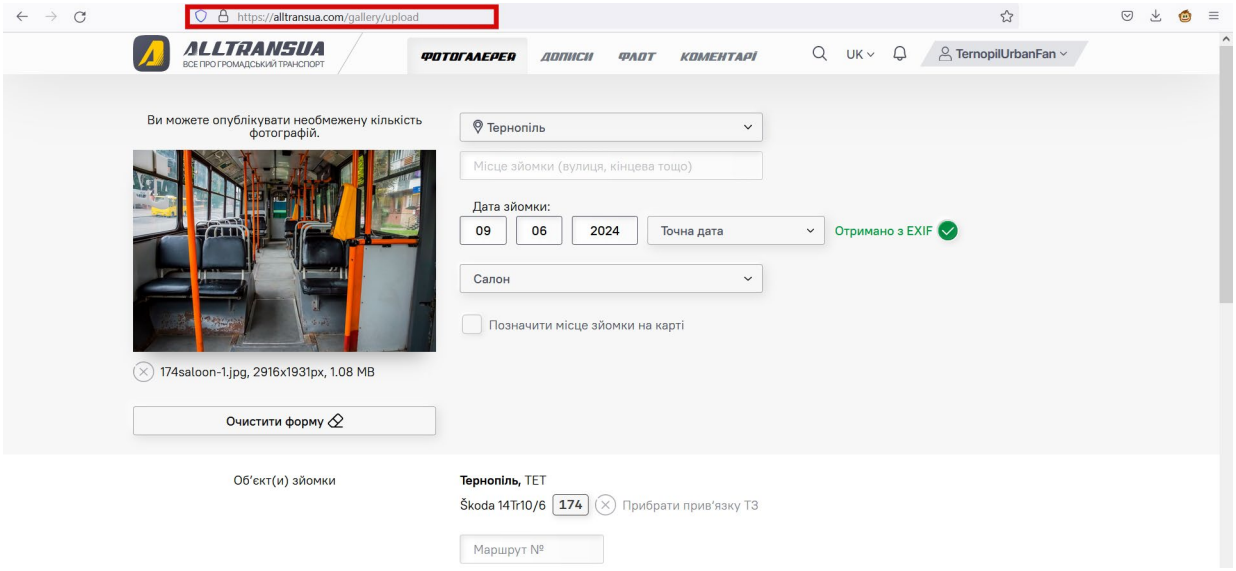

Рисунок 3.16 – Зразок дотримання КД на прикладі використання захищеного HTTPS-підключення

Таким чином, щодо вимог з дотримання Критеріїв конфіденційності, дотримано майже усіх вимог, але залишається актуальною проблема дотримання регулярного проведення обстеження сайту на наявність/відсутність каналів витоку інформації.

3.2.2 Критерії цілісності

З урахуванням тематики та функціональності транспортного ресурсу AllTransUA маємо наступні вимоги щодо дотримання вимог критеріїв цілісності:

А) Довірча цілісність (ЦД) повинна гарантувати захищеність інформації, яку публікує користувач (фотографії/дописи/коментарі) від її зміни/знищення з

боку інших користувачів сайту, а також можливості проводити модерацію контенту (коментарів/фотографій) з трьома варіантами: прийняття, відправлення на доопрацювання або відхилення.

Б) Адміністративна цілісність (ЦА) повинна забезпечувати можливість адміністраторам та локальним редакторам керувати повноваженнями користувачів і за потреби виправляти неточності, надані користувачами.

В) Відкат (ЦО) повинен гарантувати можливість скасувати операцію завантаження фотографії / їх послідовність і повернення (відкат) фотографій/коментарів до попереднього стану.

Г) Як і у випадку з КВ, згідно послуги цілісності під час обміну (ЦВ) передбачено вимога використання захищеного HTTPS-з'єднання для шифрування даних, що передаються між користувачами та сервером [12, с. 16-19].

Згідно аналізу Критеріїв цілісності маємо наступні результати:

- ЦД досягається за рахунок можливості переведення користувачів на премодерацію фото (модерацію фото зразу після публікації) та власне чинної системи модерації фото (яка може працювати і відносно користувачів, що не перебувають на премодерації фотографій, якщо хтось поскаржився на якість викладеного фотоматеріалів), яка завершується одним з трьох можливих варіантів, як на рисунку 3.17 – прийняттям фотографії до публікації, відправленням на доопрацювання або відхиленням. У випадку з модерацією коментарів це працює зовсім інакше, тобто існують лише два варіанти результатів модерації коментарів: прийняття або відхилення, адже вимога переписати коментар є доволі обтяжливою для її виконання з боку користувача-відправника (користувач не завжди може бути обізнаний щодо вимог модераторів коментарів).

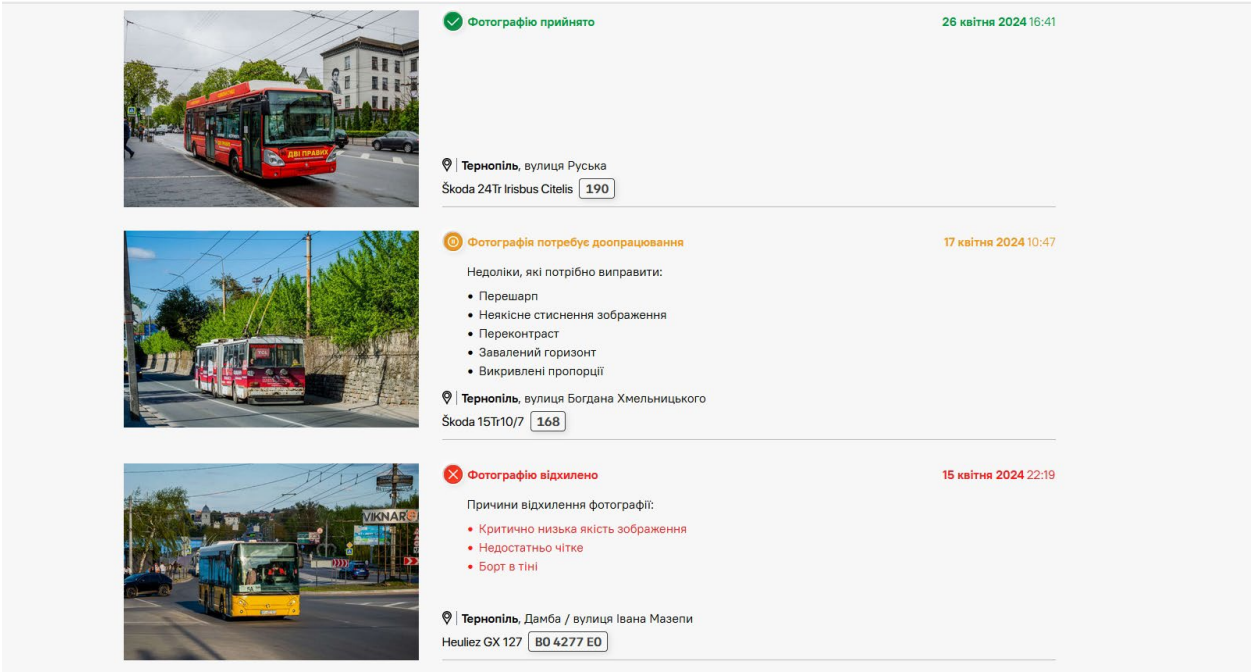

Рисунок 3.17 – Дотримання ЦД на прикладі чинної системи модерації фотоматеріалів

- ЦА досягається за рахунок наявності повноважень адміністраторів та локальних модераторів щодо виправлення неточностей, написаних в коментарях до фотографій / обговорень, а також можливості адміністраторів назначати певних користувачів на нижчі/вищі посади.

- Роль виконання вимоги ЦО грає можливість переміщення фото в чернетки: хоча користувач не може видаляти фотографію без повноважень адміністраторів/модераторів, є функція помістити фото в Чернетки, яка полягає в можливості безкінечно вносити правки (червона кнопка, яка дозволяє змінювати фотографії та/або опис до них) аж до моменту публікації фотографії (зелена кнопка), таким чином, це замінює функцію видалення і повторного завантаження, як можна бачити на рисунку 3.18 та рисунку 3.19. Також ЦО забезпечується завдяки функції самостійної заміни користувачем фотографії в перші 12 годин після публікації фотографії, навіть якщо вона не перебуває в стані модерації “Фотографія потребує доопрацювання”.

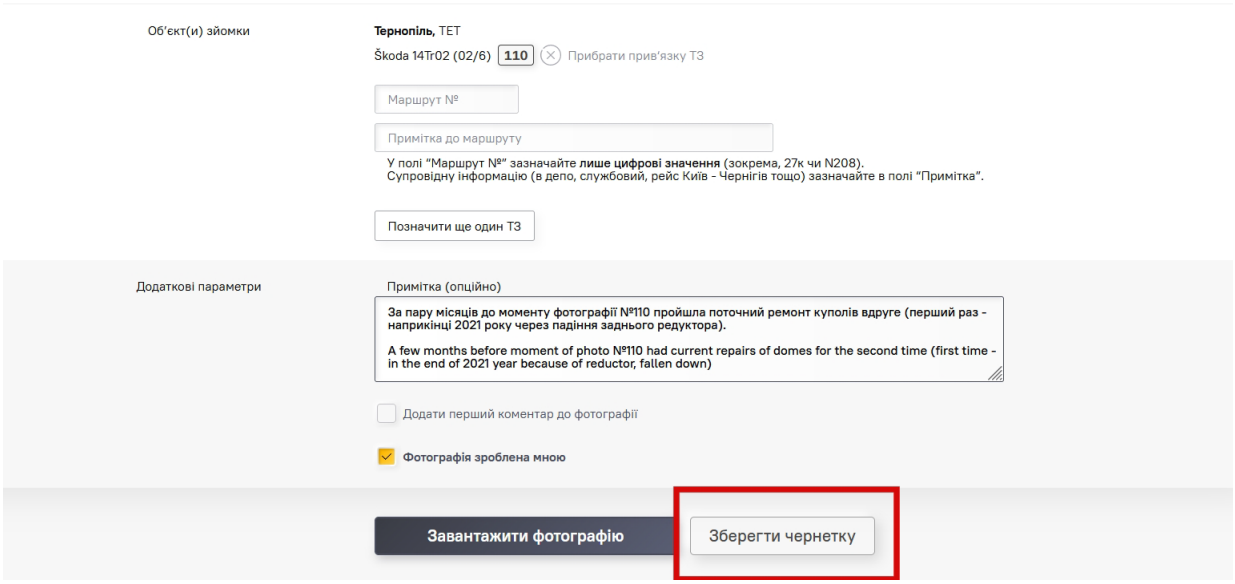

Рисунок 3.18 – Чернетки в ролі альтернативи послуги відкату (ЦО): користувач не має права самостійно видаляти фото

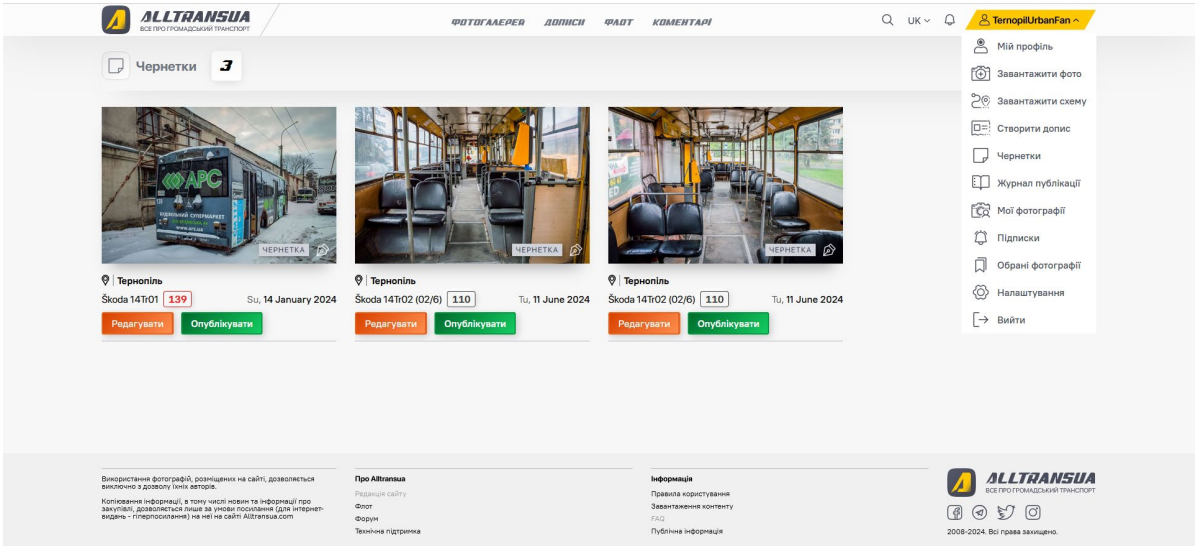

Рисунок 3.19 – Чернетки в ролі альтернативи послуги відкату (ЦО): користувач не має права самостійно видаляти фото

- Як і у випадку з КВ, ЦВ забезпечується завдяки використанню захищеного HTTPS-з'єднання, що забезпечує безпеку даних при передачі через незахищені канали (див. рисунок 3.16).

Таким чином, хоча вимогу ЦО (відкату) задовільнити прямо неможливо в випадку з інтерфейсом сайту AllTransUA, оскільки користувач не має права самостійно видаляти фотографію, проте є можливість зробити реалізацію функції ЦО опосередковано: зберігати фотографії в чернетках і працювати безкінечно, завдяки чому потреба видаляти та знову відновлювати попереднє фото (що деколи буває актуально, якщо наступне фото користувача за якістю дещо гірше за попереднє). Всі інші вимоги (ЦД, ЦА, ЦВ) сайт задовольняє також.

3.2.3 Критерії доступності

З урахуванням тематики та функціональності транспортного ресурсу AllTransUA маємо наступні вимоги щодо дотримання вимог критеріїв доступності:

А) Згідно вимоги використання об’єктів (ДР) повинна бути передбачена можливість користувачів керувати використанням послуг, які надає сайт AllTransUA.

Б) Послуга стійкості до відмов (ДС) повинна гарантувати можливості використання функціоналу сайту (окремих його компонентів) у разі відмови інших.

В) Гаряча заміна (ДЗ) повинна гарантувати доступність функціоналу сайту (на прикладі процесу завантаження фотографії) в процесі заміни контенту у разі потреби.

Г) Відновлення після збоїв (ДВ) повинне гарантувати повернення сайту до попереднього захищеного стану після відмови в роботі серверів та/або перебоїв в наданні послуг [12, с. 20-23].

Згідно аналізу Критеріїв доступності маємо наступні результати:

- ДР забезпечується завдяки широкому спектру послуг, що пропонує сайт AllTransUA, зокрема фільтрації коментарів, фотографій за різними

критеріями (місто, вулиця, автор, дата, вид транспорту, наявність/відсутність геоміток/опису, модель та інші), як вказано на рисунку 3.20 (фільтрація фото) та рисунку 3.21 (фільтрація коментарів), а також наявністю функції модерації фотографій та коментарів (див. рисунок 3.17):

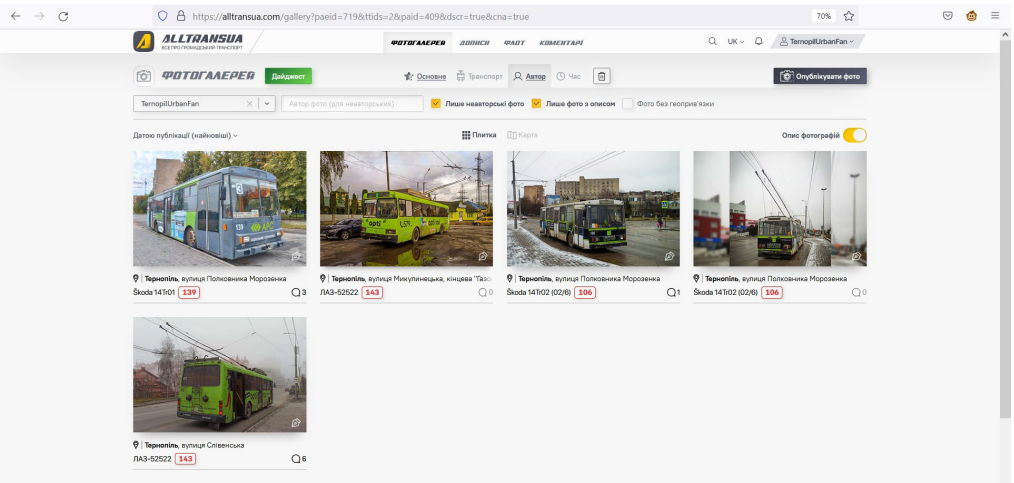

Рисунок 3.20 – ДР на прикладі можливості реалізації фільтрування фотографій за різними ознаками: встановлено фільтрацію неавторських фото, які мають опис

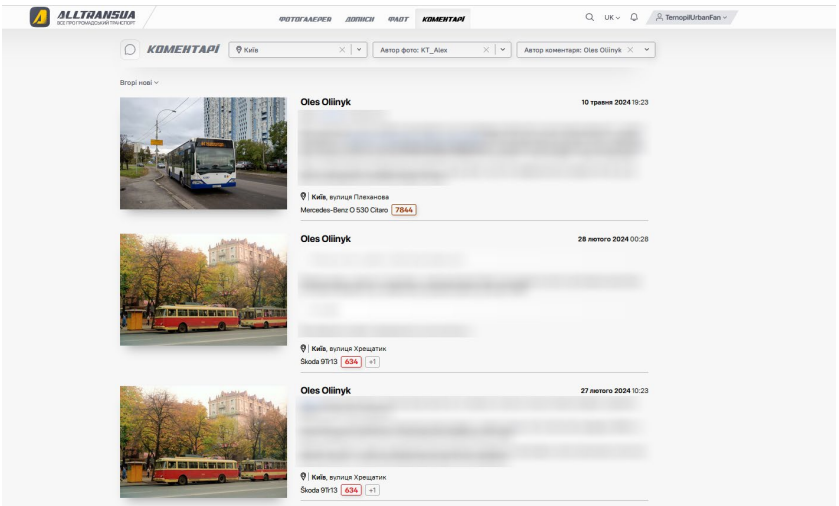

Рисунок 3.21 – ДР на прикладі можливості реалізації фільтрування коментарів за різними ознаками: встановлено фільтрацію коментарів, які залишив один користувач під фотографіями іншого користувача

- На жаль, сайтом AllTransUA послуга відмовостійкості (ДС) не передбачена – коли стається відмова сайту, спливає вікно, що повідомляє про

збій роботи всього сайту, а не лише окремого компонента, як на рисунку 3.22. Проте при завантаженні фото і публікації першого коментаря до фотографії одразу після завантаження фото деколи може виникнути помилка 400, однак саме фото завантажується одразу / потрапляє в чергу модерації, як видно на рисунку 3.23, рисунку 3.24, але публікується уже без написаного коментаря, як видно на рисунку 3.25, тож проблема відмовостійкості залишається актуальною.

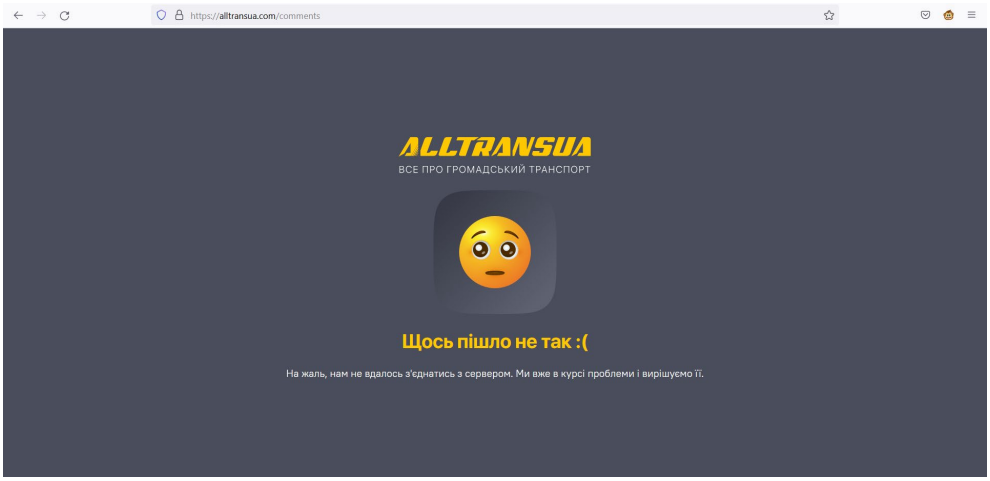

Рисунок 3.22 – Проблема відмовостійкості, що стосується не лише окремих функцій, а й усього сайту

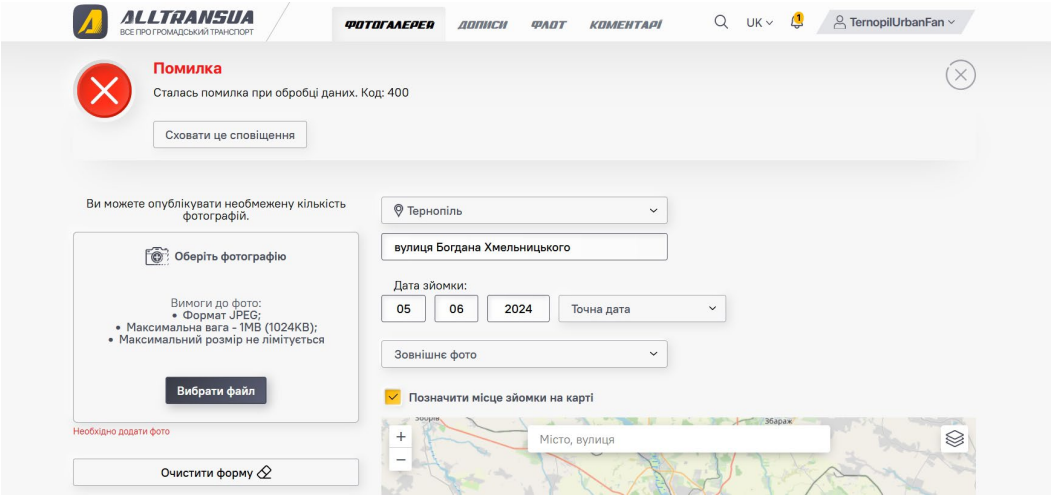

Рисунок 3.23 – Проблема відмовостійкості на прикладі збою 400 при публікації фотографії одразу з першим коментарем під нею

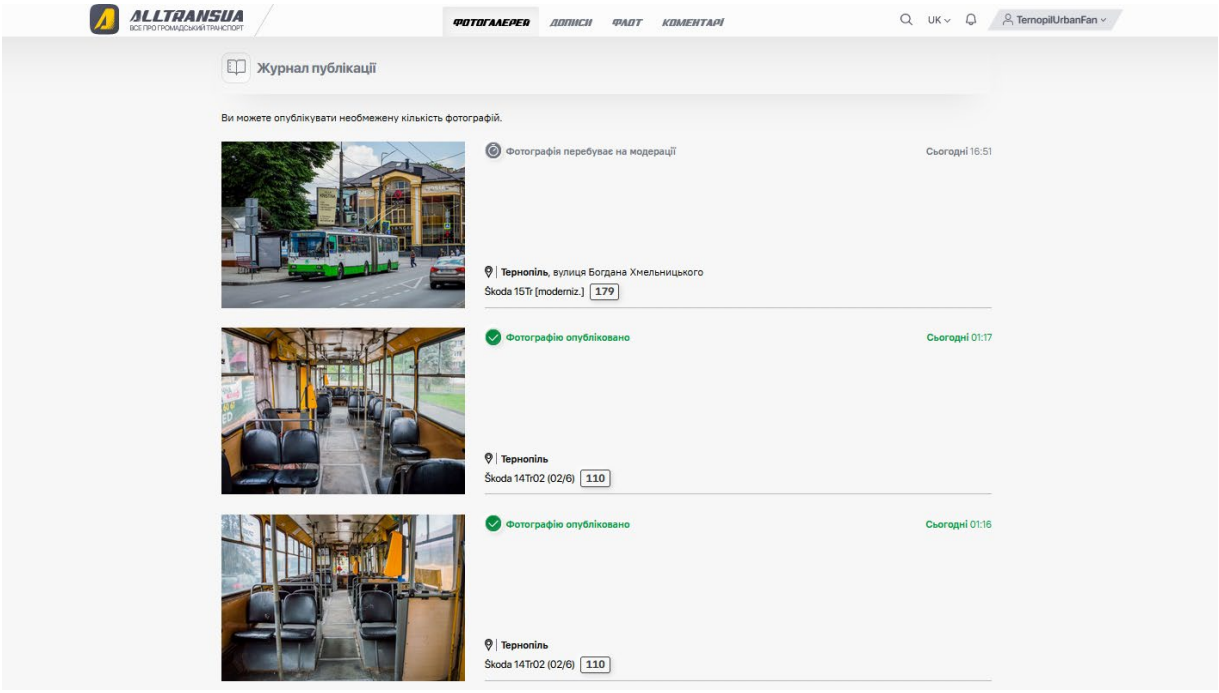

Рисунок 3.24 – Проблема відмовостійкості на прикладі збою 400: фото таки потрапило в чергу на модерацію (також відображаються в ролі опублікованих фотографії з категорії ”Чернетки”)

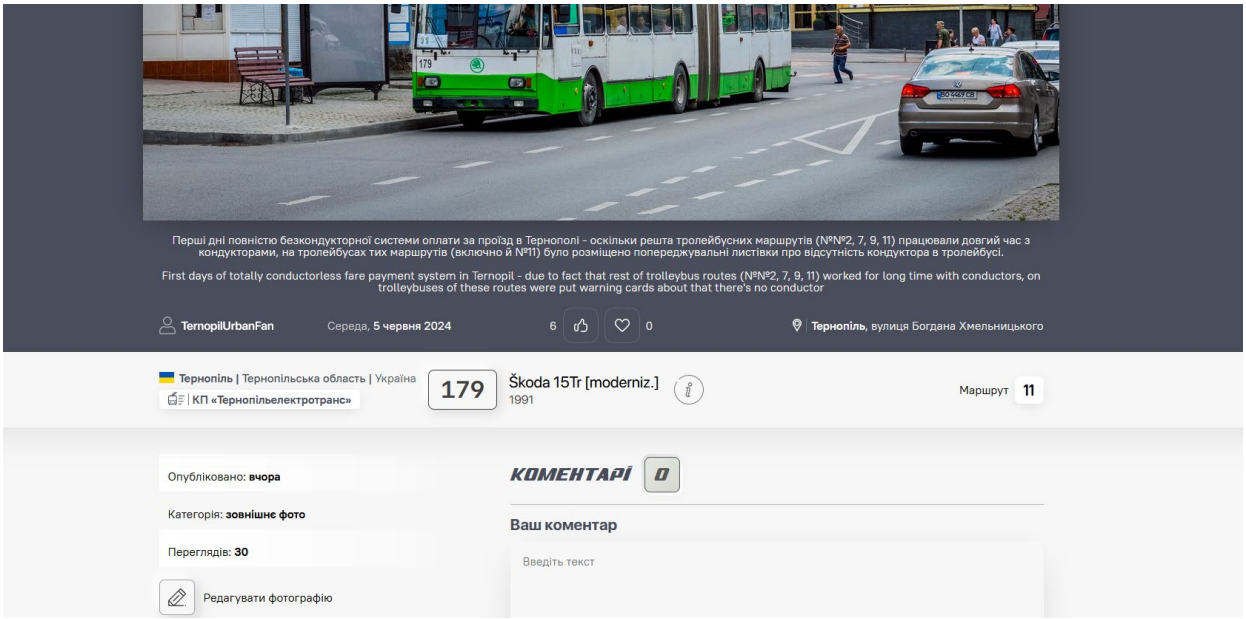

Рисунок 3.25 – Проблема відмовостійкості на прикладі збою 400: фото опубліковано, проте без коментаря

- Послугу ДЗ забезпечено завдяки можливості заміни фотографії користувача навіть без перебування його на премодерації, що діє перші 12

годин з моменту публікації фотографії, як вдалося з'ясувати в процесі комунікації з адміністраторами сайту AllTransUA, як показано на рисунку 3.26:

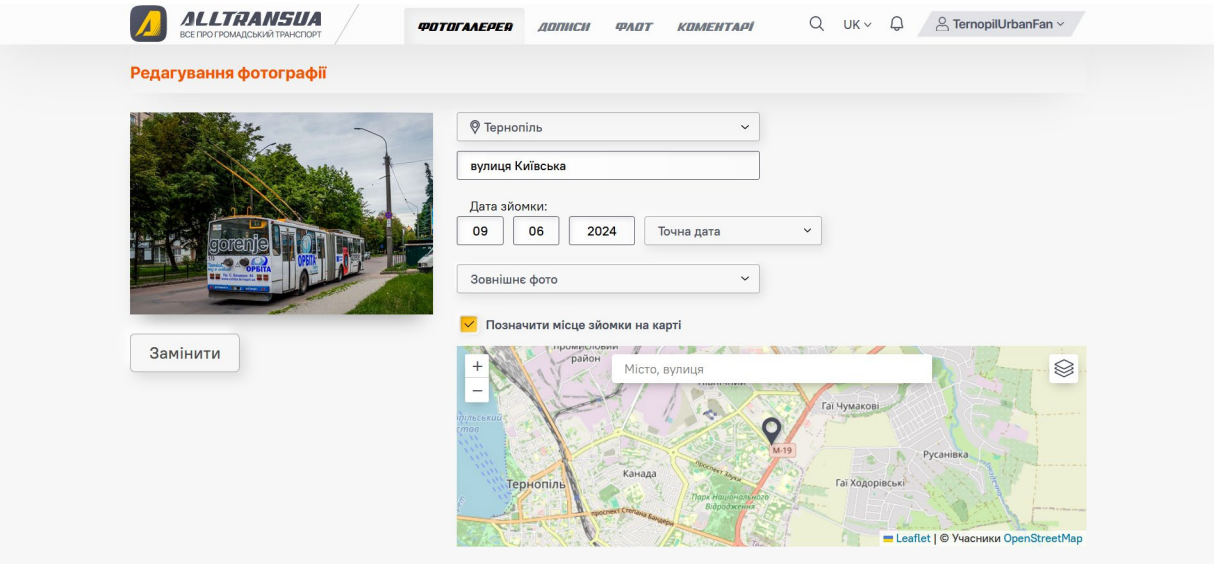

Рисунок 3.26 – ДР на прикладі можливості реалізації заміни фото протягом перших 12 годин з моменту публікації фотографії

- ДВ досягається за рахунок можливості стабільного збереження повного функціоналу сайту AllTransUA після відмов.

Таким чином, хоча більшість вимог Критеріїв доступності і забезпечено, залишається актуальною проблема відсутності відмовостійкості сайту у разі відмови хоча б одного компонента.

3.2.4 Критерії спостережності

З урахуванням тематики та функціональності транспортного ресурсу AllTransUA маємо наступні вимоги щодо дотримання вимог спостережності:

А) Послуга реєстрації (НР) повинна передбачено можливість контролювання неприйнятних для сайту AllTransUA дій, до прикладу, контроль над порушенням правил завантаження контенту.

Б) Згідно ідентифікації та автентифікації (НИ) повинна бути передбачена можливість адміністраторів сайту AllTransUA визначати та перевіряти

особистість користувачів, що намагаються отримати доступ до сайту шляхом входу в обліковий запис.

В) Згідно послуги достовірного каналу (НК) повинна бути передбачена можливість користувача взаємодіяти з персоналом сайту AllTransUA, а саме наявність різних каналів комунікації з сайтом.

Г) Розподіл обов'язків (НО) повинен гарантувати зменшення потенційних збитків від навмисних та ненавмисних (помилкових) дій користувачів та обмеження авторитарного керування, а саме повинні бути різні посади користувачів на сайті AllTransUA.

Д) Цілісність комплексу засобів захисту (НЦ) передбачає визначення рівня можливості сайту щодо самозахисту та керування захищеними об'єктами (кількістю вподобайок та супер-вподобайок, обліковими даними користувачів), що однозначно вимагає використання захищеного HTTPS-з'єднання.

Е) Самотестування (НТ) повинне передбачати можливість сайту перевіряти правильність функціонування та цілісність функціональності, якими цей сайт характеризується.

Є) Згідно послуг ідентифікації та автентифікації при обміні (НВ) даними повинно бути передбачене використання сайтом захищеного HTTPS-з'єднання.

Ж) Автентифікація відправника (НА) повинна передбачати захист від відмови від авторства і однозначне встановлення належності коментаря його користувачу сайту AllTransUA, тобто факт його створення та відправки.

З) Автентифікацією отримувача (НП) повинна бути передбачена можливість захисту відмови від факту написання користувачем коментаря шляхом його прочитання іншими користувача [12, с. 24-32].

Шляхом аналізу Критеріїв конфіденційності ми отримали наступні результати:

- НР досягається завдяки згаданій в п. 3.2.2 системі модерації фотографій та контенту.

- НИ досягається завдяки чинним механізмам ідентифікації та автентифікації, проте така система є однофакторною, як вказано на рисунку 3.27. В цілях безпеки та захищеності від злому, варто використовувати багатофакторну автентифікацію (див. пп. 3.1, с. 45-46), тому проблема ідентифікації та автентифікації залишається актуальною:

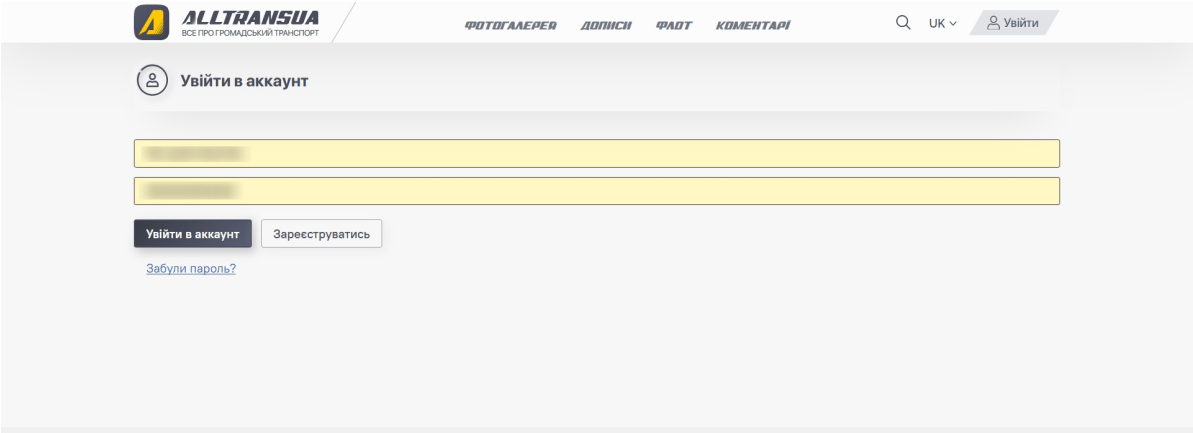

Рисунок 3.27 – Проблема ідентифікації та автентифікації на прикладі наявності лише однофакторної автентифікації

- НК досягається завдяки різноманіттю каналів зв’язку. Є акаунти сайту AllTransUA в відомих соцмережах на зразок (Facebook, Instagram), а також локальні чати сайту в Telegram (чат, що сповіщає про оновлення, що регулярно надходять та чат підтримки та комунікації з адміністраторами, модераторами та редакторами).

- Послуги НЦ і НВ задовольняються завдяки використанню сайтом AllTransUA захищеного HTTPS-підключення (рисунок 3.16).

- В ході комунікації з адміністрацією сайту було з’ясовано, що сайтом не передбачено можливість НТ (самотестування функцій), якими він характеризується (система модерації контенту, перегляд інформації про профіль користувача, можливість пошуку контенту за обраними фільтрами та інші).

- Автентифікація відправника (НА) та отримувача (НП) досягається завдяки неможливості користувача вносити правки після того, як інші

користувачі напишуть інші коментарі, тобто в такому випадку гарантується неможливість заперечення авторства коментаря шляхом його видалення, як видно на рисунку 3.28 та рисунку 3.29 (коли коментар редагувати можна):

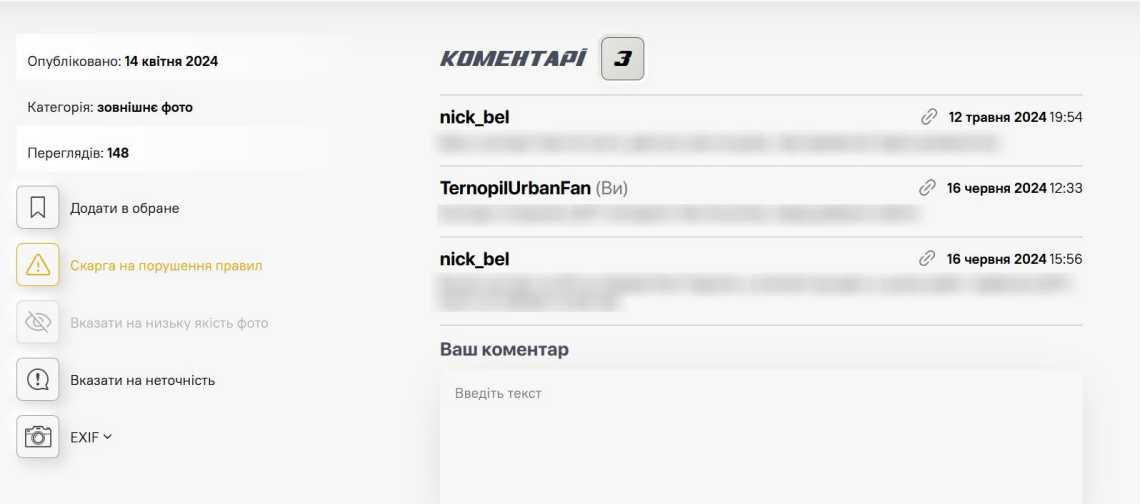

Рисунок 3.28 – Автентифікація відправника та отримувача на прикладі неможливості внесення користувачем змін в коментар після появи наступних коментарів від інших користувачів

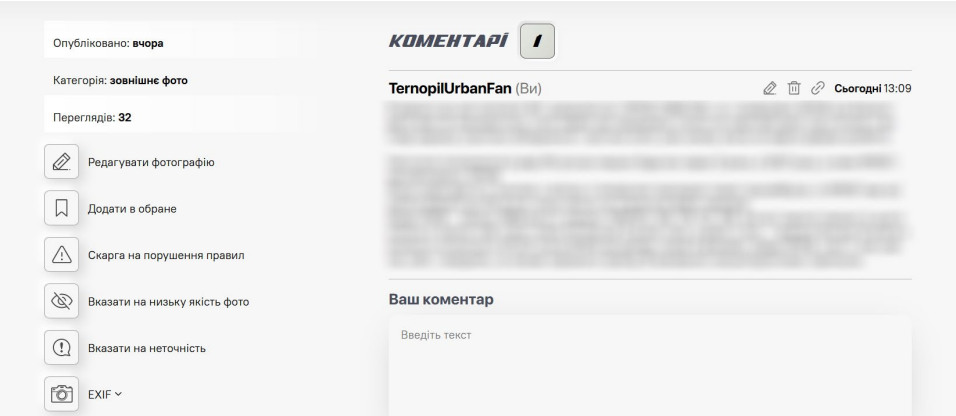

Рисунок 3.29 – Автентифікація відправника та отримувача (можливість редагування опублікованого коментаря)

Таким чином, згідно результатів перевірки на відповідність Критеріям спостережності, реалізовано майже всі вимоги, окрім двох. По-перше, потрібно впровадити багатофакторну автентифікацію, щоб запобігти НСД та створенню обхідних акаунтів (для спроб обійти блокування наявного) завдяки біометричній перевірці (відбиток пальця, сканування обличчя). По-друге,

потрібно розробити хоча б на адміністративному рівні (використовувати можуть цю функцію лише адміністратори) самотестування важливих вищезгаданих функцій сайту.

3.2.5 Критерії гарантій

З урахуванням тематики та функціональності транспортного ресурсу AllTransUA маємо наступні вимоги щодо дотримання вимог Критеріїв гарантії:

А) Вимоги до архітектури повинні гарантувати спроможність сайту AllTransUA повноцінно ввести в дію політику безпеки.

Б) Вимоги до середовища розробки повинні передбачати цілковиту керованість процесів розроблення та супроводження оцінюваного сайту з боку розробника.

В) Вимоги до алгоритмів процесу проєктування повинні гарантувати наявність точного опису та відповідності реалізації сайту вихідним вимогам (політиці безпеки) на кожній з стадій розробки.

Г) Вимоги до функціонального середовища повинні забезпечувати незмінність (відсутність несанкціонованого внесення змін) в функціонал сайту AllTransUA в процесі представлення нововведень цільовій аудиторії сайту, а також інсталяції та ініціації Замовником у відповідності до вимог розробника.

Д) Вимогами до документації передбачається надання розробником сайту AllTransUA опису послуг безпеки та настанови адміністратору та користувачу щодо послуг безпеки. Окрім цього, повинні бути викладені основні принципи політики безпеки, а також самі послуги.

Е) Випробування сайту – передбачено наступні вимоги:

- подання Розробником для перевірки програми, процедури та методики випробувань усіх механізмів реалізації послуг безпеки;

- докази тестування у вигляді детального переліку результатів тестувань;

- усунення уразливостей та повторне тестування сайту для підтвердження відсутності недоліків та нових слабких місць;

- виконання тестів на подолання механізмів захисту та доведення факту відносної або абсолютної стійкості сайту до атак з боку Розробника [12, с. 33-38].

В ході комунікації з адміністрацією з'ясувалося, що:

- оцінок архітектури на відповідність вимогам Критеріїв гарантій не проводилося;

- вимоги до середовища розробки та алгоритмів процесу проєктування, а точніше, власне процесу впровадження нововведень в сайт AllTransUA є в наявності, проте детальна оцінка на відповідність вимогам не проводилася;

- оцінювання функціонального середовища сайту на відповідність вимогам також не проводилося;

- документація щодо надання розробником опису послуг з надання безпеки та рекомендацій користувачам щодо політик безпеки також не надавалася;

- тестування функціональності сайту AllTransUA проводиться вручну адміністраторами, однак детальний перелік результатів тестувань сайту на вразливості, на стійкість до атак з боку адміністратора, який одночасно є розробником, а також програма випробувань усіх механізмів функціонування сайту не розроблялися, проте проводиться усунення недоліків.

Таким чином, щоб задовольнити повністю вимоги Критеріїв гарантій, розробникам потрібно проводити регулярно наступні заходи: оцінювання архітектури сайту, середовища розробки та функціонування на відповідність вказаним вимогам, надання розробником послуг та настанов щодо безпеки адміністраторам та користувачам, формування переліку результатів тестування функціональності сайту при кожному нововведенні в сайт (результати тестів на вразливості, програма випробувань усіх механізмів функціонування сайту, результати тестів на стійкість до загроз з боку розробника).

3.3 Висновки до третього розділу

В цьому розділі було проведено практичну реалізацію політики безпеки для сайту AllTransUA на основі обраної в другому розділі рольової політики безпеки, реалізовано модель загроз для сайту AllTransUA згідно методології STRIDE у вигляді таблиці до кожної з категорій загроз (Spoofing, Tampering, Repudiation, Information Disclosure, Denial Of Service, Elevation Of Privileges), а також проаналізовано сайт на відповідність кожному з п’яти Критеріїв оцінки захищеності автоматизованих систем згідно документу НД ТЗІ 2.5-004-99, а саме: Критеріям конфіденційності, цілісності, доступності та спостережності, а також Критеріям гарантій.

Політика безпеки передбачає можливість керування cookie-файлами, політику щодо конфіденційності користувачів, описує мету та терміни обробки та збереження особистих даних користувачів сайту AllTransUA, взаємодію сайту з іншими сайтами та третіми сторонами, гарантує безпеку для неповнолітніх користувачів сайту та комунікацію й звітність перед користувачами стосовно внесення змін в Політику безпеки. Саму політику безпеки наведено в додатку А.

В процесі моделювання загроз за методологією STRIDE, а саме розробкою таблиць загроз для кожної з вищезгаданих категорій загроз, було з’ясовано, що існуючі загрози виникають передусім завдяки відсутності багатофакторної автентифікації, що могло б забезпечити від спроб отримання зловмисником НСД та створення обхідних акаунтів в разі блокування основного. Також рекомендується впровадити політику створення паролів, яка відхилятиме легкі для вгадування паролі та уже існуючі, щоб збільшити зловмиснику час зламування пароля і впровадити перевірку щодо певності перед публікацією фотографії/коментаря/допису, щоб запобігти ненавмисній публікації користувачами власних облікових даних або/та програмного коду, включно й уразливого.

В процесі аналітики сайту AllTransUA на відповідність Критеріям оцінки захищеності інформаційних ресурсів з’ясувалося, що попри відповідність сайту більшості з вимог, є певні недоліки, які слід доопрацювати в процесі розробки, а саме: потрібно регулярно проводити обстеження сайту на наявність каналів витоку інформації (Критерії конфіденційності), для остаточного задоволення вимог Критеріїв доступності потрібно забезпечити можливість функціонування окремих функцій сайту (фільтрація контенту, публікація і модерація фото/коментарів, пошук по флоту та інші), для виконання вимог Критеріїв спостережності реалізувати хоча б на адміністративному рівні самотестування важливих вищезгаданих функцій сайту, а для забезпечення виконання вимог Критеріїв гарантій адміністрація сайту повинна проводити регулярно оцінювання архітектури сайту, середовищ розробки та функціонування на відповідність поставленим вимогам, вести власний перелік результатів тестування функцій сайту щоразу, коли вводиться нововведення в сайт.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Охорона праці та безпека життєдіяльності при роботі з ПК

Закони та нормативні акти з охорони праці розробляються і імплементуються для захисту працівників і підвищення їх добробуту. Незалежно від контексту робочого середовища важливість забезпечення здоров'я і безпеки на робочому місці для всіх тепер стала реальністю і гарантовано Конституцією України та іншими нормативними актами. Цей факт справедливий і для сектора ІТ, оскільки сфера розробки ПЗ чи сайтів є одним з секторів, які також несуть ризики з точки зору гігієни праці і техніки безпеки [13].

В даному розділі опишемо охорону праці в галузі розробки і використання ПЗ.

Охорона праці — це система законодавчих актів, соціально-економічних, організаційних, технічних, гігієнічних і лікувально-профілактичних заходів і засобів, забезпечуючих безпеку, охорону здоров’я і працездатність людини в процесі праці.

На працюючих в кабінеті адміністраторів впливають ті ж фактори, що і в будь-якій іншій галузі промисловості - захворюваність, умови та характер праці тощо.

Так як адміністратор буде використовувати ПК, то особливої шкоди його здоров’ю він не несе, лише варто дотримуватись правильної організації робочого місця при роботі за ПК.

Важливим елементом організації праці на підприємстві є вдосконалення планування, організація і обслуговування робочих місць з метою створення на кожному з них необхідних умов для високопродуктивної праці.

Робочі місця класифікують за такими параметрами, як професія та кількість виконавців, ступінь спеціалізації, рівень механізації, кількість устаткування, характер розміщення в просторі.

Залежно від кількості виконавців розрізняють індивідуальні та колективні робочі місця. Індивідуальне робоче місце призначене для роботи одного працівника протягом зміни. Колективне робоче місце призначене для здійснення процесу праці одночасно кількома робітниками (бригадою).

Робоче місце адміністратора фірми (організації) оснащене комп'ютерним столом і офісним кріслом. На столі розміщений комп'ютер, який включає системний блок, монітор, клавіатуру, мишку, колонки.

Освітленість робочого місця працівників повинна відповідати оптимальним установленим нормам, які визначаються характером і розрядом по ступені точності, характеристики фону й контрасту об'єкта розходження [13].

Раціональне освітлення приміщень є одним з основних факторів по попередженню травматизму й професійних захворювань працівників. У приміщеннях використовують як природне, так і штучне освітлення.

Штучне освітлення може бути загальне, місцеве й комбіноване. Як загальне освітлення приймаються освітлювальні прилади, установлені під стелею виробничого приміщення й вони освітлюють більшу площу. Як місцеве освітлення приймаються освітлювальні прилади, установлені безпосередньо на робочому місці працівника, і які освітлюють тільки робоче місце. При комбінованому освітленні використовується й місцеве, і загальне освітлення. Найчастіше використовується комбіноване освітлення.

4.2 Вимоги безпеки при роботі на ПК

Під час роботи за комп'ютером виконувати всі вимоги інструкції.

Працювати з клавіатурою, мишею тільки чистими руками. На клавіші натискати плавно, без різких ударів. У випадку виникнення несправностей повідомити вищестоячого керівника. Забороняється самостійно регулювати апаратуру чи ремонтувати.

Не дозволяється використовувати ряд переносок і вмикати їх одна в одну. При виникненні загоряння необхідно використовувати вогнегасник.

Вимоги безпеки в аварійних ситуаціях:

1. При появі незвичного звуку або відімкненні апаратури негайно припинити роботу, доповісти директору.

2. При появі запаху паленого слід припинити роботу, вимкнути апаратуру.

3. При потраплянні під напругу знеструмити робоче місце, повідомити керівництво, при потребі надати першу медичну допомогу.

Правила експлуатації ПК:

При можливості підключити до ПК прилад безперервного живлення (UPS), що дає можливість роботи комп'ютерів при повному відключенні електроживлення від 5 хвилин до декількох годин (у залежності від сили приладу). За цей час можна закінчити роботи на комп'ютері, щоб при його включенні не була втрачена інформація.

Всі кабелі, які з'єднують системний блок ПК з іншими приладами, потрібно вставити і виймати тільки при вимкненому комп'ютері.

Встановити монітор так, щоб було зручно дивитись (дивитись на екран потрібно під прямим кутом, трохи зверху вниз, екран повинен бути злегка нахилений, нижній його край повинен бути ближче до вас.

Необхідно обережно використовувати дискети (акуратно вставляти у дисковод, не можна гнути, стискати, доторкатися руками до відкритих ділянок магнітного покриття).

Засоби надання долікарської допомоги потерпілим від електричного струму:

- При ураженні людини електричним струмом необхідно як найшвидше звільнити її від дії струму. Тому перше, що повинен зробити той, хто надає допомогу — швидко вимкнути (знеструмити) електроустановку.

- Для вивільнення потерпілого від дротів чи частин, якими йде струм, треба користуватися сухим одягом, канатом, палицею, дошкою чи будь-яким іншим сухим предметом, що не проводить електричний струм.

- Якщо потерпілий у свідомості, а перед цим був у непритомному стані чи довгий час під струмом, його треба покласти в зручне положення і до прибуття лікаря забезпечити йому цілковитий спокій.

- Якщо потерпілий перебуває в непритомному стані, проте в нього збереглися стійке дихання і пульс, його треба рівно й зручно покласти, розстебнути одяг і забезпечити цілковитий спокій. При цьому давати нюхати нашатирний спирт, розтирати і зігрівати тіло.

- При відсутності дихання чи пульсу в потерпілого допомога повинна бути спрямована на відновлення життєвих функцій шляхом штучного дихання і поверхневого (непрямого) масажу серця.

- Починати штучне дихання слід відразу після вивільнення потерпілого від електричного струму. Найефективнішим способом проведення штучного дихання є спосіб «з рота в рот» і «з рота в ніс».

- Поверхневий масаж здійснюється методом ритмічних стискувань серця через передню стінку грудної клітини.

- Для проведення поверхового масажу серця потерпілого треба покласти на спину, на щось тверде, розстебнути одяг, що затрудняє дихання.

- Натискування слід проводити швидким поштовхом і повторювати його приблизно один раз на секунду.

- Для забезпечення організму достатньою кількістю повітря при зупинці серця слід одночасно з масажем серця проводити й штучне дихання способом вдування повітря в легені потерпілого.

- Співвідношення між штучним диханням і закритим масажем серця повинно бути 1:5.

- При появі ознак життя поверховий масаж і штучне дихання слід продовжувати ще впродовж 5—10 хвилин, так, щоб вдування співпадало з моментом власного вдиху потерпілого.

4.3 Висновки до четвертого розділу

В даному розділі розроблено рекомендації щодо реалізації охорони праці та безпеку життєдіяльності при розробці та вдосконаленні ПЗ, які передбачають ті ж фактори, що і в будь-якій іншій промисловій галузі: захворюваність, умови та характер праці.

Охорона праці включає в себе законодавчі, соціально-економічні, організаційно-технічні, технічні, гігієнічні та лікувально-профілактичні заходи, спрямовані на забезпечення безпеки та здоров’я розробників, що займаються розширенням функціоналу сайту AllTransUA. У кабінетах адміністраторів важливо дотримуватися раціональної організації робочого місця, що передбачає належний рівень освітлення та ергономіку.

Згідно правильної експлуатації ПК передбачено підключення джерел безперебійного живлення в цілях надання можливості зберегти важливу інформацію, також потрібно дотримуватися правил підключення кабелів, поводження з дискетами та іншими носіями інформації.

Дотримання вимог безпеки при роботі з ПК вимагає чистих рук, плавних натискань на клавіші, заборону щодо самостійного ремонту обладнання та використання ряду переносок та правильне використання електропристроїв, щоб не перенавантажувати мережу. У разі небезпечних ситуацій необхідно проінформувати керівників про несправності, що виникли та за потреби надати першу медичну допомогу. Надання домедичної допомоги складається з таких заходів: знеструмлення потерпілих, використання сухих предметів для їх звільнення від дії струму, проведення штучного дихання та поверхневого

масажу серця. Забезпечення правильного дихання та пульсу потерпілого є ключовими цілями до моменту прибуття лікарів.

Таким чином, охорона праці в ІТ-галузі спрямована на створення безпечних умов праці, попередження виробничих травм та надання своєчасної домедичної допомоги у разі виникнення надзвичайних ситуацій.

ВИСНОВКИ

В даній кваліфікаційній роботі було проведено аналіз загроз для інформаційно-пізнавального транспортного ресурсу AllTransUA з подальшим викладенням рекомендацій щодо покращення безпеки сайту, було здійснено перевірку сайту та його функціоналу на відповідність вимогам нормативного документа НД ТЗІ 2.5-004-99 (надалі – Критерії), а також викладено політику безпеки сайту AllTransUA, з якою студенти можуть ознайомитися в додатку А.

В ході досліджень було виявлено, що найкраще для сайту підходить методологія побудови загроз STRIDE, оскільки інші моделі загроз або орієнтовані на невеликі підприємства (OCTAVE), або стосуються безпосередньо бізнес-цілей, що несумісно з цілями сайту, який не є комерційним (PASTA та TRIDE), або охоплюють не весь процес життєдіяльності сайту (VAST).

В процесі аналітики моделі загроз, оформленої у вигляді таблиці для кожної з шести категорій, було розроблено рекомендації щодо впровадження багатофакторної автентифікації, надійної політики паролів та впровадження перевірки певності у власних діях, що дозволить забезпечити сайту AllTransUA зменшення ймовірності виникнення загроз, що виникли з вини чиєїсь недбалості, імовірності реалізації НСД до облікових записів користувачів/адміністраторів та створення обхідних облікових записів.

Завдяки аналітиці сайту AllTransUA та його функціоналу на відповідність Критеріям було встановлено висновки щодо відповідності сайту встановленим вимогам та рекомендації, які можуть допомогти зробити захищене середовище розробки, забезпечити відмовостійкість сайту та виявити канали витоку інформації і усунути їх.

Студенти зможуть ознайомитися з політиками безпеки, методологіями побудови моделі загроз, власне НД ТЗІ 2.5-004-99, деякими з функцій сайту AllTransUA і використати їх в подальшій комунікації з його адміністраторами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021, March). Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. In Journal of Physics: Conference Series (Vol. 1840, No. 1, p. 012026). IOP Publishing.

2. Lupenko, S., Orobchuk, O., & Xu, M. (2019, September). Logical-structural models of verbal, formal and machine-interpreted knowledge representation in Integrative scientific medicine. In Conference on Computer Science and Information Technologies (pp. 139-153).

3. Revniuk O.A., Zagorodna N.V., Kozak R.O., Karpinski M.P., Flud L.O. "The improvement of web-application SDL process to prevent Insecure Design vulnerabilities". Applied Aspects of Information Technology. 2024; Vol. 7, No. 2: 162–174. DOI: https://doi.org/10.15276/aait.07.2024.12.

4. Стебельський, М., & Букатка, С. (2023). Загальносистемні криптографічні політики ОС Linux. Порівняльний аналіз. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання ", 177-178.

5. Tymoshchuk, V., Dolinskyi, A., & Tymoshchuk, D. (2024). MESSENGER BOTS IN SMART HOMES: COGNITIVE AGENTS AT THE FOREFRONT OF THE INTEGRATION OF CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS. Матеріали конференцій МЦНД, (07.06. 2024; Луцьк, Україна), 266-267. https://doi.org/10.62731/mcnd-07.06.2024.004

6. Тернопільський національний технічний університет ім. Івана Пулюя. Ролева політика безпеки. *Wiki ТНТУ*. URL: https://wiki.tntu.edu.ua/Ролева_політика_безпеки (Дата звернення: 08.06.2024).

7. Allen-Addy C. Threat Modeling Methodology: STRIDE. *IriusRisk*. URL: https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride (Дата звернення: 09.06.2024).

8. Allen-Addy C. Threat Modeling Methodology: TRIKE. *IriusRisk*. URL: https://www.iriusrisk.com/resources-blog/trike-threat-modeling-methodologies (Дата звернення: 09.06.2024).

9. Allen-Addy C. Threat Modeling Methodology: OCTAVE. *IriusRisk*. URL: https://www.iriusrisk.com/resources-blog/octave-threat-modeling-methodologies (Дата звернення: 09.06.2024).

10. Allen-Addy C. Threat Modeling Methodology: PASTA. *IriusRisk*. URL: https://www.iriusrisk.com/resources-blog/pasta-threat-modeling-methodologies (Дата звернення: 09.06.2024).

11. What Is Threat Modeling. *Wind Driver*. URL: https://www.windriver.com/solutions/learning/threat-modeling (Дата звернення: 09.06.2024).

12. НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: Нормативний документ від 28.04.1999 р. № 806: станом на 28 груд. 2012 р. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf (Дата звернення: 10.06.2024).

13. Павлов Е.В. Охорона праці в охороні здоров'я. – Луцьк: Книжковий світ, 2022 (Дата звернення: 21.06.2024).

ДОДАТКИ

Додаток А Політика безпеки інформаційного ресурсу AllTransUA

AllTransUA ставиться з повагою до конфіденційності вашого особистого життя

Захист конфіденційності вашої приватної галузі під час обробки особистих даних та процесу роботи з інформаційними ресурсами сайту (БД, форуми, публікації дописів) і захист облікових даних транспортних підприємств є для нас важливим завданням, яке враховується в наших процесах постійного доопрацювання функціоналу транспортного ресурсу AllTransUA. Особисті дані, що збираться під час відвідин транспортного пізнавального онлайн-ресурсу ми обробляємо конфіденційно та лише згідно норм чинного законодавства. Захист даних та інформаційна безпека є частиною нашої корпоративної політики.

Загальні положення Сайту AllTransUA

Ми з повагою ставимося до конфіденційної інформації, що належить особам, що відвідали наш Сайт https://alltransua.com/, а також тих, хто користується наданими Сайтом послугами, наприклад, використання фотоматеріалів для написання дописів в засобах масової інформації, соцмережах (незареєстровані Користувачі), завантажує фотоматеріали і доповнює бази даних, бере участь в покращенні та розширенні функціоналу нашого Сайту (зареєстровані Користувачі). Власне через це ми прагнемо захищати конфіденційну інформацію (персональні дані, сукупність відомостей про ідентифікованих фізичних осіб та тих, які можуть бути ідентифікованими, тим самим забезпечивши якомога зручніші умови для використання запропонованих Сайтом послуг для кожного з Користувачів.

Дана Політика конфіденційності та захисту персональних даних (надалі – “Політика”) визначає порядок обробки та види особистих даних (дата народження, ім'я, електронна пошта, на яку записано обліковий запис Користувача, місце проживання), ціль використання цих даних, взаємодію з третіми особами, заходи з безпеки для захисту особистих даних, а також надання Користувачем персональних даних з ціллю отримання доступу до ресурсів Сайту, а також внесення змін у видимій для інших Користувачів персональній інформації (додавання або видалення), а також вирішенні питань щодо захисту особистих даних.

Погодження обробки особистих даних

Користувачі підтверджують свою згоду на обробку персональних даних, наданих в процесі входу / реєстрації, а саме: опис профілю, справжнє ім'я користувача та його нікнейм, дату народження, електронну пошту, до якої прив'язаний обліковий запис та паролі.

Звертаємо увагу користувачів Сайту AllTransUA

Сайт обмежується збором мінімального обсягу інформації, необхідного виключно для задоволення запиту суб'єкта особистих даних. У разі запиту необов'язкової для надання інформації Користувач буде повідомлений про необов'язковість надання такої інформації в момент її збору.

Сайт гарантує вільне використання фотоматеріалів та інформації з дописів поза його межами лише за умови посилання на використані інформаційні ресурси, проте дозволяє перегляд фотоматеріалів та публічних обговорень згідно закону України "Про доступ до публічної інформації”.

Сайт не збирає і не толерує збирання будь-якої інформації будь-ким з Користувачів, щодо обробки якої законодавством встановлено певні вимоги,

зокрема, інформації про расове або етнічне походження, політичні, релігійні та світоглядні переконання, участь в політпартіях та профспілках, судимості, а також даних про здоров’я, біометричні та генетичні показники згідно статті 7 закону України "Про захист персональних даних”.

Обробка та зберігання персональних даних

Обробка та зберігання даних користувачів інформаційного ресурсу AllTransUA здійснюються в онлайн-дата-центрах, де розміщені плагіни та інше допоміжне ПЗ, відповідальне за функціональність сайту. Надані персональні дані за бажання Користувача можуть зберігатися в базі особистих даних.

Мета використання особистих даних

Особисті дані використовуються для забезпечення функціонування Сайту (завантаження Користувачами власних фотографій, створення дописів, публікації коментарів в форумах-обговореннях на різну тематику), керування правами доступу Користувачів згідно наявних привілеїв та вдосконалення комунікації з користувачами і функціоналу Сайту.

Термін зберігання особистих даних

Особисті дані зберігаються протягом терміну, не більшого за потрібний для їх обробки час.

Після того, як суб’єкт особистих даних перестає бути Користувачем шляхом блокування його облікового запису (зокрема, численних порушень правил завантаження контенту (завантаження контенту без погодження правовласника, публікація неправдивих відомостей) та публікації коментарів, що суперечать правилам Сайту, зокрема, перехід на особистості, образи,

приниження, дискредитація за соціальною, релігійною та іншими ознаками, персональні дані та контент, завантажений Користувачем, залишаються в відкритому доступі, а суб'єкт автоматично переходить в стан незареєстрованого Користувача з обмеженими можливостями. При спробі входу в обліковий запис виникає повідомлення про його блокування Адміністрацією Сайту.

Використання cookie-файлів

Cookie-файл – це файли з певним обсягом інформації, що відправляються веб-браузеру, з якого було здійснено вхід в Сайт та зберігаються на пристрої Користувача, на якому було здійснено вхід в Сайт (портативний/стаціонарний ПК, мобільний телефон, планшет та інші пристрої).

Розрізняють постійні файли (зберігаються вічно) та тимчасові сесійні файли cookie (зберігаються до певного моменту, наприклад, закриття браузера чи вимкнення можливості зберігати файли cookie).

Важливо розуміти наступне:

- Файли cookie оновлюються при повторних відвідинах Сайту
- Навіть у разі блокування облікового запису (порушення Користувачем правил поведінки на Сайті) файли cookie зберігаються
- В більшості випадків веб-браузери дозволяють автозбереження файлів cookie на пристрої Користувача

Сайт AllTransUA передбачає перелік таких категорій файлів cookie:

- строго необхідні файли cookie – використовуються в разі реєстрації/входу на Сайт, як показано на рисунку А.1 (запит на збереження файлів cookie) та рисунку А.2 (демонстрації факту збереженості файлів cookie) на прикладі браузера Opera:

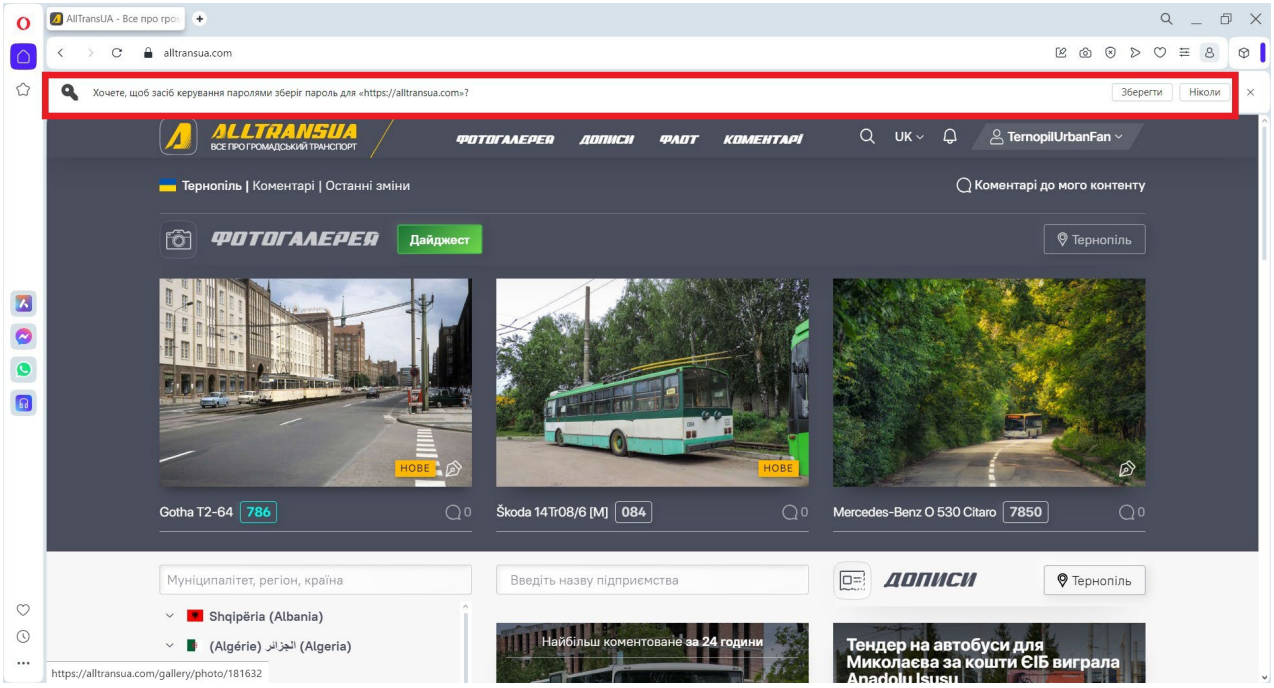

Рисунок А.1 – Запит браузером Opera на збереження файлів cookie

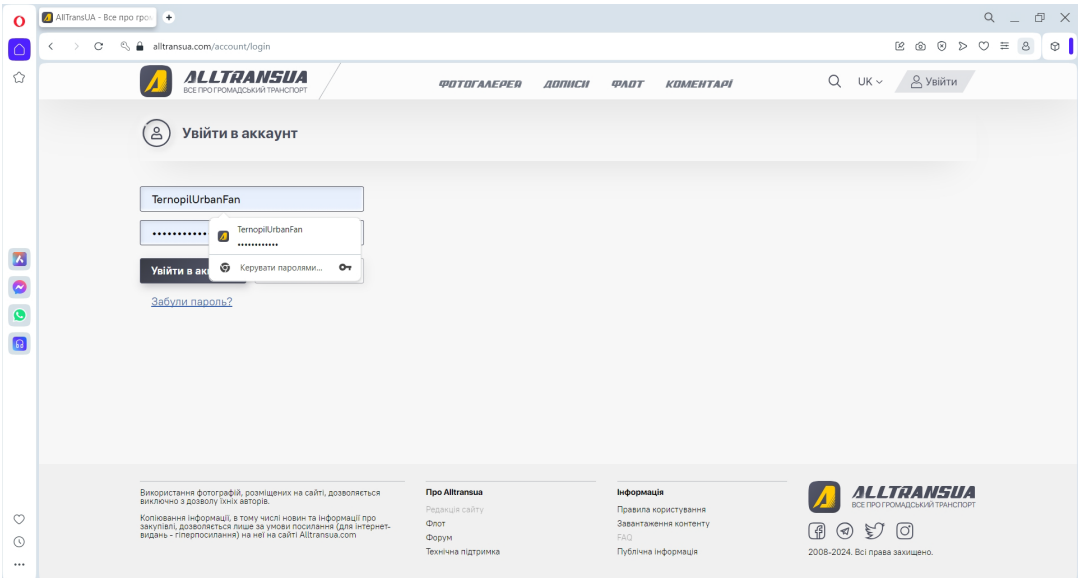

Рисунок А.2 – Суворо необхідні файли cookie при вході в інтерфейс користувача сайту AllTransUA

- експлуатаційні файли cookie – використовуються у разі здійснення пошуку по Сайту AllTransUA (пошуку одиниць ТЗ по бортовому або державному номеру, пошуку фотографій по назві користувача), вставлення

приміток до фотографій в процесі їхнього завантаження, як показано на рисунку А.3 та рисунку А.4:

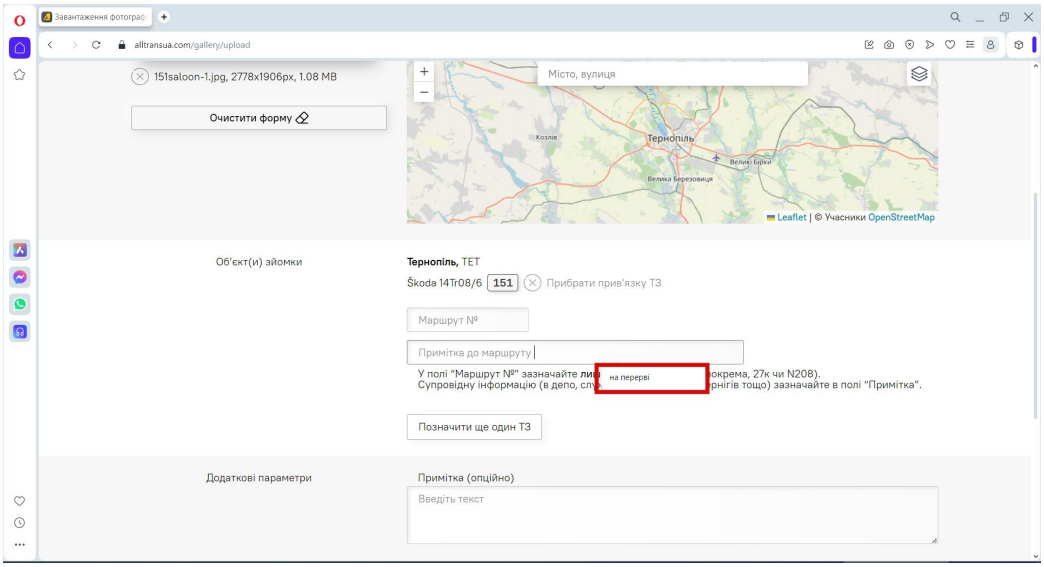

Рисунок А.3 – Експлуатаційні файли cookie на прикладі додаткової інформації, яка міститься на завантажуваній фотографії

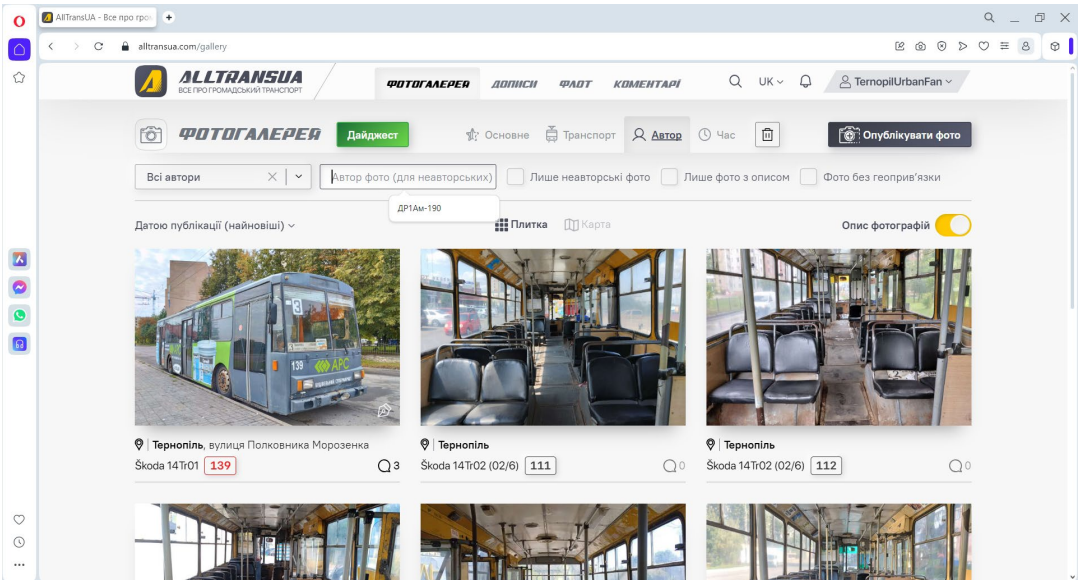

Рисунок А.4 – Експлуатаційні файли cookie на прикладі пошуку фотографій за автором, який не є зареєстрованим на сайті

Як бачимо, з ціллю зробити швидшим та простішим процес входу в сайт та роботу з завантажуваними фотоматеріалами, зазначені файли cookie запам’ятовують надану Користувачем інформацію, щоб підвищити

ефективність взаємодії з інтерфейсом Сайту AllTransUA, як показано на прикладі браузера Opera.

Керування файлами cookie

Основні веб-браузери налаштовані на автозапам'ятовування та записування файлів cookie, проте їх можна вимкнути, можна скористатися довідкою в браузері або шляхом натискання клавіші F1:

- Microsoft Edge: https://privacy.microsoft.com/uk-ua/privacystatement
- Mozilla Firefox: https://www.mozilla.org/uk/privacy/websites/cookie-settings/
- Chrome: https://support.google.com/chrome/answer/95647?hl=uk
- Opera: https://help.opera.com/en/latest/web-preferences/#cookies

Важливо розуміти, що:

- зміна налаштувань файлів cookie може виглядати дещо інакше на веб-браузерах мобільних пристроїв;

- можливість повноцінної роботи AllTransUA є лише за умови використання cookie-файлів;

- вимкнення cookie може призвести до обмеження доступу до контенту AllTransUA та неповноцінної його функціональності.

У разі умисного видалення файлів cookie з веб-браузера під час подальших відвідин Сайт буде пропонувати Користувачеві ввімкнути та використовувати файли cookie, а інформація про користувачів, надана за допомогою цих файлів, не підлягає продажу та поширенню на загальний доступ і є власністю Сайту.

Взаємодія AllTransUA з іншими ресурсами

Під час використання користувачем сервісів на сторінці Сайту можуть бути присутніми посилання на інші сторінки та облікові записи третіх осіб на інших інтернет-ресурсах, що означає, що ці інтернет-ресурси можуть отримувати та працювати з інформацією про ваше відвідування цих сторінок, а також іншу інформацію, що передає браузер Користувача. Такими ресурсами можуть бути:

- соцмережі (Facebook, Instagram, Telegram);
- засоби масової інформації, на які посилаються Користувачі в дописах, фотографіях та коментарях;
- інші фотосховища;
- інші транспортні інформаційно-пізнавальні ресурси.

Безпека неповнолітніх Користувачів

Сайт призначено для Користувачів всіх вікових категорій, в тому числі неповнолітніх та малолітніх. Втім, Сайт має жорстку політику щодо фільтрації контенту і безпеки осіб, які не досягли повноліття, тобто Сайтом передбачено заборону на публікацію чутливого контенту, ввічливе, неупереджене ставлення до усіх Користувачів AllTransUA та дотримання цензури в коментарях до обговорень та фотоматеріалів, а також вимогу до об’єктивності інформації.

Взаємодія AllTransUA з третіми особами стосовно персональних даних

Сайт не передає і не толерує передавання особистих даних третім особам, крім випадків, передбачених Законом, тобто за проханням суб’єкта персональних даних або в інших випадках.

На Сайті можна розміщувати посилання на інші веб-сайти (ЗМІ, інші фотоматеріали, бази даних, сайти розпродажу трнаспортних засобів, включно й іноземного походження), проте виключно в інформаційних цілях. Політика на інші сайти при переадресації не розповсюджується. Сайт радить ознайомитися з політикою конфіденційності, перш ніж передавати персональні дані, які ідентифікують вас.

Конфіденційність активності суб'єкта особистих даних на AllTransUA

Відомості про активність Користувачів захищено відповідно до чинного законодавства. Таким чином, гарантується захищеність таємниці активності Користувача під час його використання сервісів Сайту.

Захист особистих даних

Сайтом передбачено використання загальноприйнятих стандартів технологічно-операційного інформаційного захисту даних від втрат, змін, неправильного використання або знищення, а також дотримання обов’язків щодо дотримання конфіденційності та різних заходів безпеки для уникнення НСД, незаконного розголошення або нанесення шкоди такій інформації. Попри всі зусилля щодо захисту інформації, Сайт не гарантує відсутність ризику виникнення загроз, що мають зовнішнє спрямування.

Доступ до інформації та особистих даних надається лише привілейованим Користувачам ресурсу AllTransUA, а саме Адміністраторам, які дали згоду на нерозголошення такої інформації. Поширення особистих даних без згоди суб’єкта персональних даних дозволяється лише у випадках, передбачених законом і лише в інтересах нацбезпеки, добробуту та дотримання прав людини.

Права суб'єкта особистих даних

Сайтом передбачається, що суб’єкти особистих даних мають право на доступ до своїх особистих даних, їхнє виправлення, приховування або видалення, а також право знати механізми оброблення особистих даних, відхиляти згоду на це, застосовувати засоби захисту в разі порушень вимог щодо захисту даних, вимагати виправлення, якщо інформація про Користувача була неправильно поданою.

Внесення змін в Політику

Політика безпеки може періодично та без попереднього повідомлення Користувачів змінюватися та доповнюватися, особливо якщо було внесено зміни в законодавстві.

У разі суттєвої зміни в Політиці на Сайті буде повідомлено детально про терміни введення в чинність внесених змін. У разі, якщо до вказаного терміну Користувач не оформить письмово про незгоду з змінами в Політиці, це автоматично означатиме згоду з відповідними змінами в Політиці. Від імені Адміністрації наполегливо радимо переглядати політику, щоб бути обізнаними щодо внесених змін та доповнень.