Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Розробка архітектури системи безпеки для сайту краудсорсингової транспортної спільноти AllTransUA"

Виконав: студент (ка) VI курсу, групи СБм-61

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Завадський Костянтин Сергійович
підпис (прізвище та ініціали)

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

Нормоконтроль Стадник М. А.
підпис (прізвище та ініціали)

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

Рецензент Луцик Н. С.
підпис (прізвище та ініціали)

м. Тернопіль – 2025

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)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Завадському Костянтину Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка архітектури системи безпеки для сайту краудсорсингової транспортної спільноти AllTransUA

Керівник роботи Козак Руслан Орестович, кандидат технічних наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » 11 2025 року № 4/7-1024

2. Термін подання студентом завершеної роботи 19.12.2025

3. Вихідні дані до роботи Функціональні аспекти сайту (система модерації контенту, публікація контенту, механізми реєстрації та входу, система скарг), дослідження в галузі багатофакторної автентифікації, перевірки на метадані та журналювання даних

4. Зміст роботи (перелік питань, які потрібно розробити)
1 Структурований аналіз сайту AllTransUA, 1.1 Публікація матеріалів, 1.2 Фільтрація контенту, 1.3 Ієрархія ролей та аналіз сайту, 1.4 Система модерації, 1.5 Журналювання, 1.6 Системи реєстрації, автентифікації та авторизації, 1.7 Канали комунікації AllTransUA, 2 Аналіз джерел досліджень в обраних галузях та вразливостей сайту AllTransUA, 2.1 Аналіз досліджень в галузі багатофакторної автентифікації, 2.2 Аналіз досліджень в галузі перевірки на метадані (розпізнання об'єктів на фото), 2.3 Аналіз досліджень в галузі журналювання даних, 2.4 Аналіз вразливостей кожного з безпекових аспектів системи, 2.4.1 Публікація матеріалів та система модерації 2.4.2 Журналювання 2.4.3 Системи реєстрації, автентифікації та авторизації, 3 Формування проєкту системи безпеки сайту AllTransUA, 3.1 Побудова системи безпеки сайту AllTransUA на основі вразливостей, 3.1.1 Багатофакторна автентифікація та політика паролів, 3.1.2 Аналіз контенту на мета-дані, 3.1.3 Журналювання подій: прозора зміна привілеїв, 3.1.4 Побудова загального проєкту системи безпеки, 4 Охорона праці та безпека життєдіяльності, 4.1 Охорона праці і правила протипожежної безпеки, 4.2 Безпека життєдіяльності офісних працівників, Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Теслюк В.М., проректор з адміністративно–господарської роботи та будівництва		

7. Дата видачі завдання 19.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	19.09 – 22.09	Виконано
2.	Підбір джерел для виконання кваліфікаційної роботи магістра	22.09 – 30.09	Виконано
3.	Детальна аналітика функціоналу транспортного ресурсу AllTransUA	02.10 – 15.10	Виконано
4.	Опрацювання джерел в галузі дослідження	15.10 – 22.10	Виконано
5.	Формулювання розділу «Структурований аналіз сайту AllTransUA»	26.10 – 02.11	Виконано
6.	Формулювання розділу «Аналіз джерел досліджень в обраних галузях та вразливостей сайту AllTransUA»	03.11 – 15.11	Виконано
7.	Побудова системи безпеки сайту AllTransUA для кожного з досліджених аспектів безпеки окремо	16.11 – 26.11	Виконано
8.	Побудова загального проєкту системи безпеки сайту AllTransUA	28.11 – 01.12	Виконано
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	02.12 – 12.12	Виконано
10.	Нормоконтроль	12.12 – 16.12	Виконано
11.	Перевірка на плагіат	16.12 – 18.12	Виконано
12.	Попередній захист кваліфікаційної роботи	18.12 – 19.12	Виконано
13.	Захист кваліфікаційної роботи	22.12.2025	

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

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

АНОТАЦІЯ

Розробка архітектури системи безпеки для сайту краудсорсингової транспортної спільноти AllTransUA // ОР «Магістр» // Завадський Костянтин Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2025 // С. 85, рис. – 52, табл. – 1, кресл. – 0, додат. – 1.

Ключові слова: AllTransUA, краудсорсингова платформа, багатофакторна автентифікація, метадані, журналювання, модерація, система скарг, контент, ієрархія ролей.

Кваліфікаційна робота присвячена розробці проєкту системи безпеки краудсорсингової платформи AllTransUA, що грунтується на основі аналізу функціональних компонентів сайту та на дотримання практик безпеки, аналізу поточної ситуації з безпекою інформації на згаданій медіа-платформі.

У ході дослідження проаналізовано літературні джерела, присвячені згаданим в ході аналізу сайту аспектам безпеки, а також розроблено загальний та проєкт системи захисту для кожного функціонального компонента, що може бути запропонований адміністраторам для втілення їх з ціллю подальшого запобігання зловживанням з боку окремих користувачів.

Отримані результати формують розуміння у адміністраторів щодо подальшого вдосконалення функціоналу сайту та підтверджують, що для захисту користувацьких даних від зламу та спроб отримання несанкціонованого доступу вкрай важливо реалізувати багатофакторну автентифікацію. Зважаючи на можливість публікувати будь-які фотографії завдяки постмодерації, що існує за замовчуванням, також важливо впровадити перевірку фотографій на метадані. Також для запобігання зловживанням важливо вдосконалити прозорість змін даних. Згадані нововведення гарантуватимуть вдосконалення рівня безпеки користувацьких даних на сайті AllTransUA.

ABSTRACT

Security system architecture development for the crowdsourcing transport community website AllTransUA // Thesis of educational level "Master"// Kostiantyn Zavadskyi // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-61 // Ternopil, 2025 // p. 85, figs. 52, tbls. 1, drws. 0, apps. 1.

Keywords: AllTransUA, crowdsourcing platform, multifactoral authentification, metadata, logging, moderation, report system, content, role hierarchy.

The qualification work is dedicated to the security system project development for crowdsourcing platform site AllTransUA, based on in-depth analysis of site's functional components and compliance with security practices, analysis of the current situation with the security of information circulating on the mentioned media platform.

During the research, literary sources were analyzed (related to functional and security aspects mentioned during in-depth site analysis), and there were developed security system projects for each functional component and a general security system project that can be proposed to administrators for their implementation in order to further prevent user abusements.

The obtained results form consideration among administrators about further site's functionality improvement and confirm that multi-factor authentification is extremely important to protect user data against hacking and unauthorized access attempts. Considering ability to publish any photos because of postmoderation existing as default, it is also important to implement photo metadata verification. Also in order to prevent power abuse, it is important to improve data editing transparency. The aforementioned innovations can guarantee an improved user data security level on the AllTransUA site.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БФА — багатофакторна автентифікація

БД — база даних

ГТ — громадський транспорт

НСД — несанкціонований доступ

ВСТУП

Актуальність теми. Система модерації, наявна на транспортній медіа-платформі AllTransUA, має невід'ємну роль в фільтрації контенту, що завантажується на сайт. В контексті модерації є вкрай важливим забезпечення можливості фільтрувати контент, що спрямований на дискредитацію конкретних осіб та/або протирічить чинному законодавству України. На сайті реєструються щоденно нові користувачі – в такому разі вкрай важливо передбачити ризик створення нових користувачів, які зареєструвалися з ціллю або обійти блокування попереднього акаунта, або свідомо нехтувати правилами етики на сайті та завантажувати дискредитаційний або незаконний контент, а в такому разі вкрай важливим є впровадження прив'язки всіх облікових записів до єдиного біометричного параметра, тобто впровадження багатофакторної автентифікації (надалі – БФА). Також існує ієрархія ролей на сайті (адміністратори, модератори, редактори і прості користувачі), а отже і можливість підвищення/зниження привілеїв користувачам, що в свою чергу, породжує потребу в прозорості, тобто журналюванні змін привілеїв, щоб запобігти упередженому ставленню адміністрації відносно користувачів сайту та прихованому зловживанню привілеями.

Мета і задачі дослідження. Метою кваліфікаційної роботи є формування проєкту системи безпеки сайту, що грунтується на структурованому аналізі безпекових аспектів сайту AllTransUA, формуванні оцінки поточного рівня захищеності даних на сайті, дослідженні вразливостей чинної системи модерації та чинних механізмів реєстрації і входу, аналізі журналювання даних на сайті. Дослідження спрямоване на покращення безпекової ситуації, спрощення роботи фотомодераторам сайту AllTransUA в фільтрації фотоконтенту, що завантажується регулярно на сайт, забезпечити прозорість та справедливість змін привілеїв на сайті AllTransUA та знизити ризик зловживання згаданим адміністративним ресурсом.

Завданням дослідження є розробити проєкт системи захисту даних та прав користувачів, поданий у вигляді кінцевих рекомендацій для вдосконалення

безпеки та функціоналу сайту, зокрема: втілення БФА, політики паролів, перевірки зображень на метадані та вдосконалення журналювання подій.

Об’єкт дослідження. Об’єктом дослідження є система модерації (премодерація і постмодерація), журналювання подій, механізми реєстрації та входу.

Предмет дослідження. Предметом дослідження є сайт краудсорсингової платформи AllTransUA.

Наукова новизна одержаних результатів кваліфікаційної роботи. Краудсорсингові ресурси було досліджено багатьма вченими, зокрема Калініною Г. М., Карим О. І., Панасом Я. В. (проблеми краудсорсингу), а також Ворожейкіним О. О, Лялюк А., Рейкіним В., Савчук Я. та іншими. Було вперше проведено аналіз наявних механізмів безпеки на основі багаторічного досвіду користування краудсорсинговою платформою AllTransUA, а також визначено дані для БФА згідно проведених досліджень у відповідній тематиці.

Практичне значення одержаних результатів. Результати, одержані в ході виконання наукового дослідження, можуть бути використані в процесі комунікації з адміністраторами сайту AllTransUA для покращення інформаційної безпеки сайту. БФА надасть змогу захистити облікові записи користувачів від спроб отримання НСД та запобігти спробам обходу блокування і створенням нових акаунтів з ціллю подальших порушень правил користування сайтом. Система перевірки на метадані може спростити роботу модераторам з фільтрації контенту (прийняття рішень стосовно прийняття / відправлення на доопрацювання / відхилення фото). Прозорість змін привілеїв забезпечить належне функціонування адміністрації сайту AllTransUA із зменшенням ризику зловживання адмінресурсом і неможливість приховано змінювати привілеї.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на XIII науково-технічній конференції «Інформаційні моделі, системи та технології».

Публікації. Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 СТРУКТУРОВАНИЙ АНАЛІЗ САЙТУ ALLTRANSUA

Доволі важливою складовою існування будь-яких додатків, включно і транспортних на прикладі досліджуваного транспортного додатка AllTransUA, є безпека користувацьких даних та самого сайту.

Для подальшого розуміння, як формувати стратегію побудови надійної системи захисту користувацьких даних краудсорсингового (від англійських слів crowd – натовп та sourcing – джерело) транспортного додатка AllTransUA, потрібно передусім провести коротку аналітику основних його аспектів.

AllTransUA як транспортний додаток, складається з наступних функціональних компонентів, серед яких основними є можливість публікації контенту (фотографії, чернетки, дописи, коментарі, форуми), система модерації контенту, яка поділяється в свою чергу на премодерацію (модерація з моменту завантаження контенту) і постмодерацію (модерація відбувається після публікації контенту), а також системи журналювання даних, системи входу та реєстрації.

1.1 Публікація матеріалів

На транспортному додатку (хоча знімок екрану зроблений на сайті, проте його функціонал не відрізняється від функціоналу додатка) передбачено можливість публікувати фотографії різних категорій (зовнішні фото, фото салонів, кабіни, заводських табличок, неідентифіковані фотографії, детальна зйомка), як на рис. 1.1:

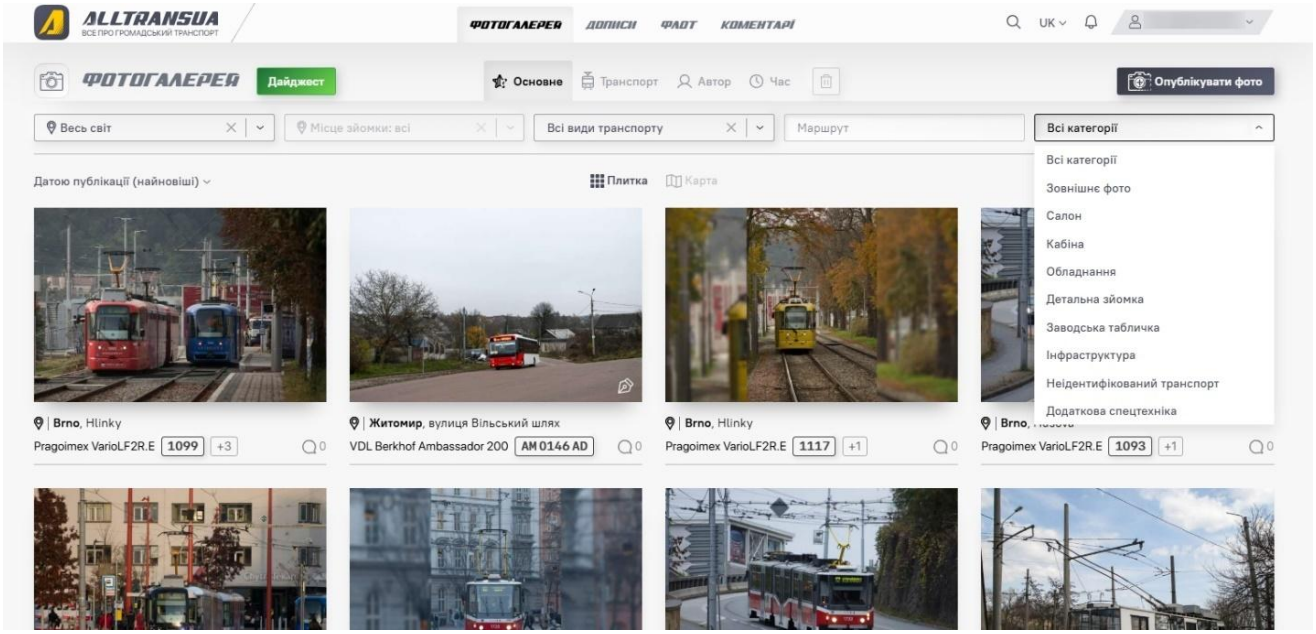


Рисунок 2.1 – Загальний принци здійснення UDP flood атаки

Чернетки передбачені передусім для того, що якщо користувач має бажання викласти фото, але з тих чи інших причин (тимчасова відсутність дозволу на публікацію, бажання уникнути публікації одноманітного контенту з однаковим місцем зйомки, відсортування менш пріоритетних фото, невпевненість в коректно вказаній інформації) тимчасово не публікує, то все ж зберігся зміст допису/фотографії, особливо якщо обсяг інформації доволі великий на прикладі допису про підсумки громадського транспорту Тернополя за 2024 рік на рисунку 1.2:

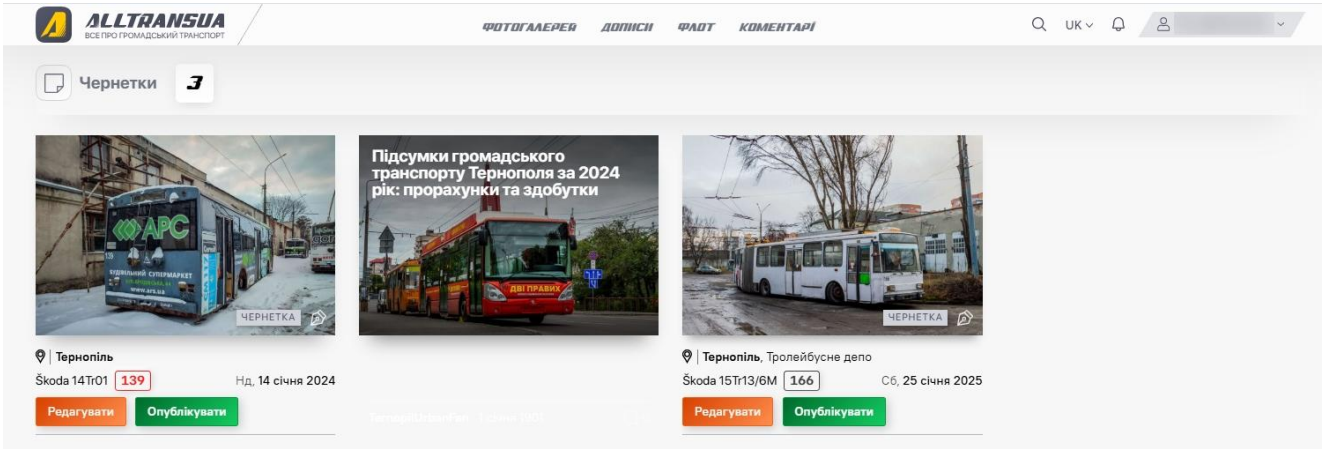


Рисунок 1.2 – Розміщення контенту в чернетках (дописи та фотографії)

Категорія “Дописи” може використовуватися користувачами в різних цілях, зокрема оприлюднення новин, пов’язаних з громадським транспортом, дослідження в галузі загальної історії транспорту/підприємства, підведення місячних/піврічних/річних підсумків, публікація різних буклетів на тему громадського транспорту (надалі – ГТ) як зображено на рис. 1.3:

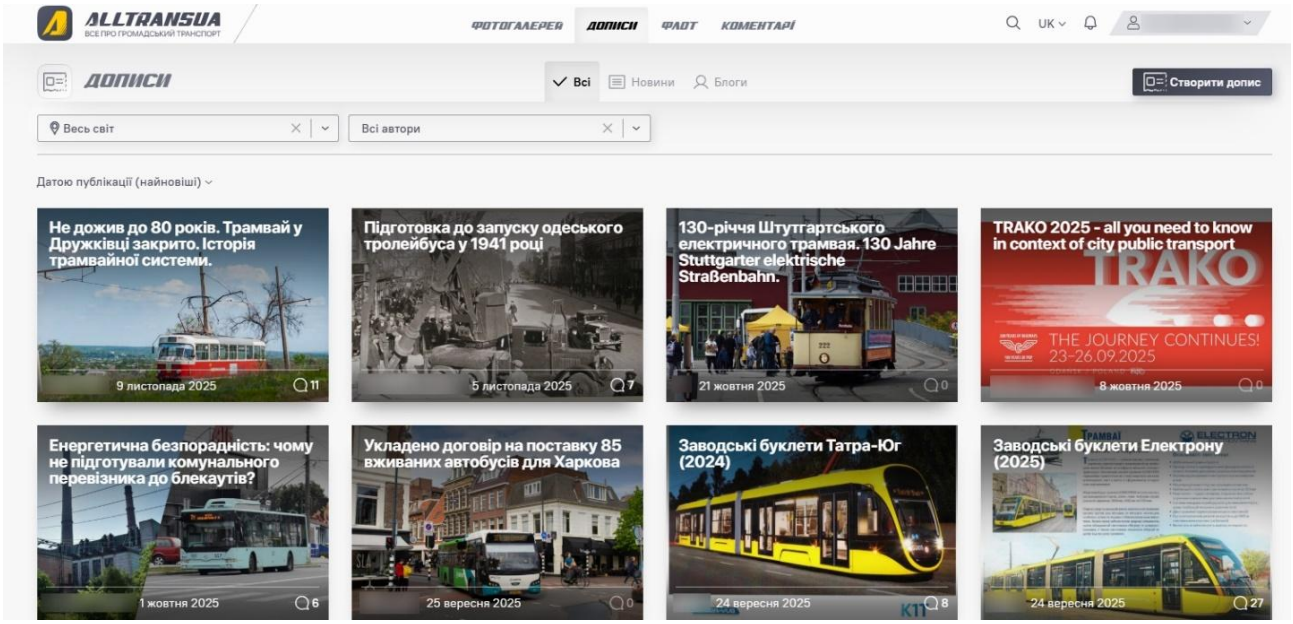


Рисунок 1.3 – Публікація дописів на різну тематику

На форумах публікуються дописи, пов’язані з конкретною тематикою, зокрема з ціллю відсортувати дописи та зручного пошуку потрібної інформації. Серед них є як і форуми з підтримки (низька інтенсивність наповнення контенту), форуми, присвячені конкретним подіям (наприклад, замовні поїздки на спеціально передбачених для цього одиницях ГТ), так і локальні форуми, що стосуються конкретних міст, як на рис. 1.4:

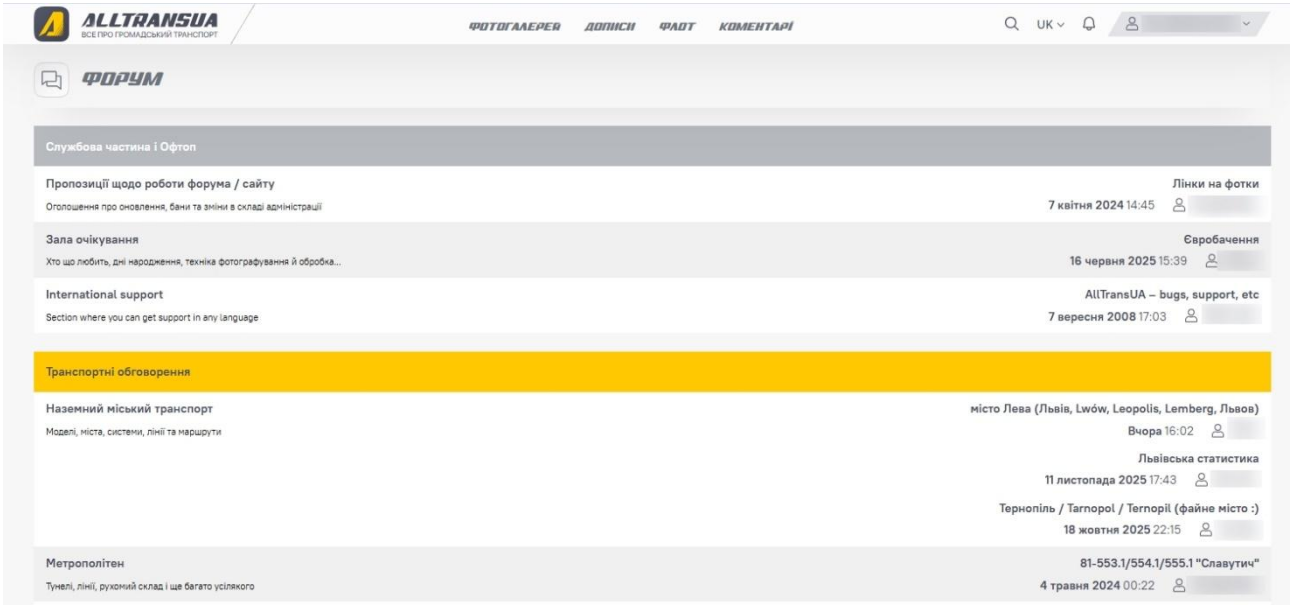


Рисунок 1.4 – Перелік форумів різної категорії: технічні (зверху) та місцеві (знизу)

Користувачі також можуть залишати під фотографіями та дописами коментарі різного характеру, якщо вони, звісно, не суперечать правилам, описаним на сайті AllTransUA, як на рисунку 1.5 (проте редагувати їх можна лише доти, доки не було залишено інший коментар):

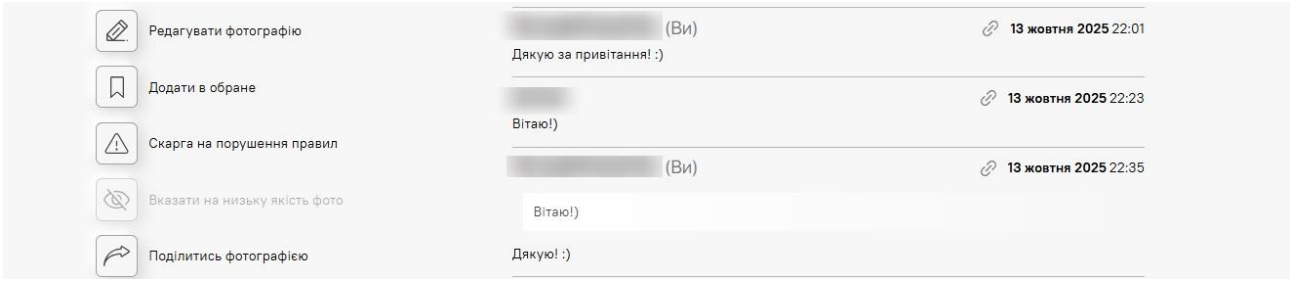


Рисунок 1.5 – Розміщення коментарів

Окрім цього, також є можливість проводити відбір контенту за різними характеристиками, як зазначено в наступному підрозділі

1.2 Фільтрація контенту

На сайті існує фільтрація контенту, яка в свою чергу поділяється на такі підвиди: фільтрація фотографій, фільтрація коментарів, фільтрація флоту та фільтрація дописів.

Функція фільтрації фотоконтенту надає змогу здійснювати пошук за наступними параметрами:

- загальні параметри (пошук фотографій, зроблених на територіальних одиницях різного рівня (місто, область, країна), місце зйомки, пошук фотографій за видом транспорту (трамвай, тролейбус, автобус, метрополітен, фунікулер та інші), за маршрутом, за вищезгаданими в пп. 1.1 категоріями фото (зовнішнє фото, салон, кабіна, заводська табличка, детальна зйомка, неідентифікований транспорт, обладнання та інші)

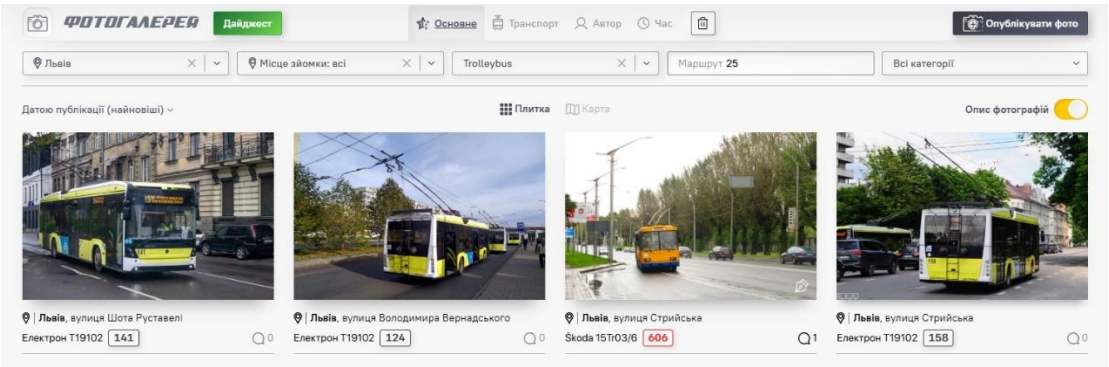


Рисунок 1.6 – Фільтрація фотографій за загальними характеристиками

- за транспортними характеристиками: даними транспортного засобу (надалі – ТЗ), зокрема за моделлю транспорту, бортовим номером, містом, підприємством

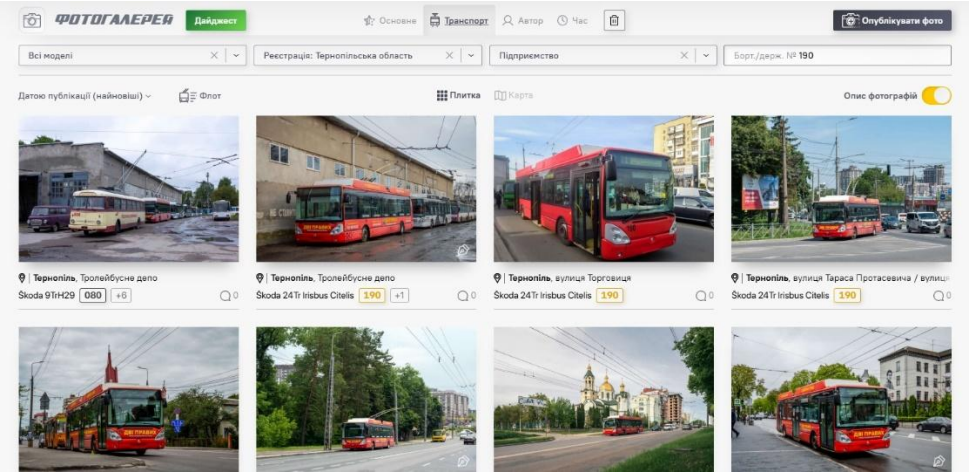


Рисунок 1.7 – Фільтрація фотографій за транспортними даними

- за авторськими параметрами: автором фотографій (безпосереднім автором фотографії), автором неавторських фото, власник яких не зареєстрований на сайті AllTransUA, за наявністю/відсутністю опису на фото, наявністю/відсутністю вказаного місця зйомки, пошуком всіх фотографій / виключно неавторських фото

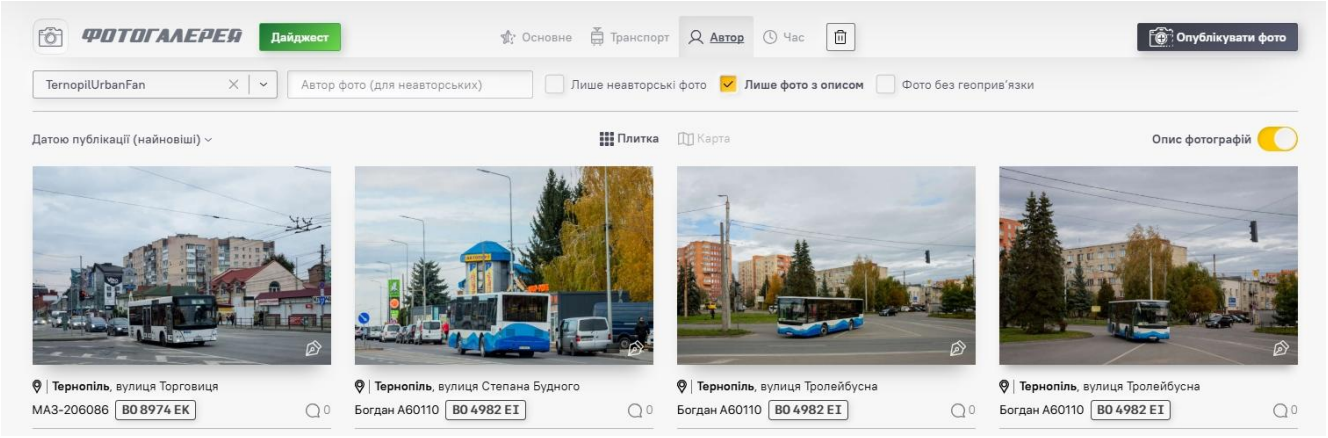


Рисунок 1.8 – Фільтрація фотографій за авторськими характеристиками

- за часовими характеристиками: пошук фотографій за датою зйомки та публікації, в тому числі і через часові інтервали зйомки та публікації

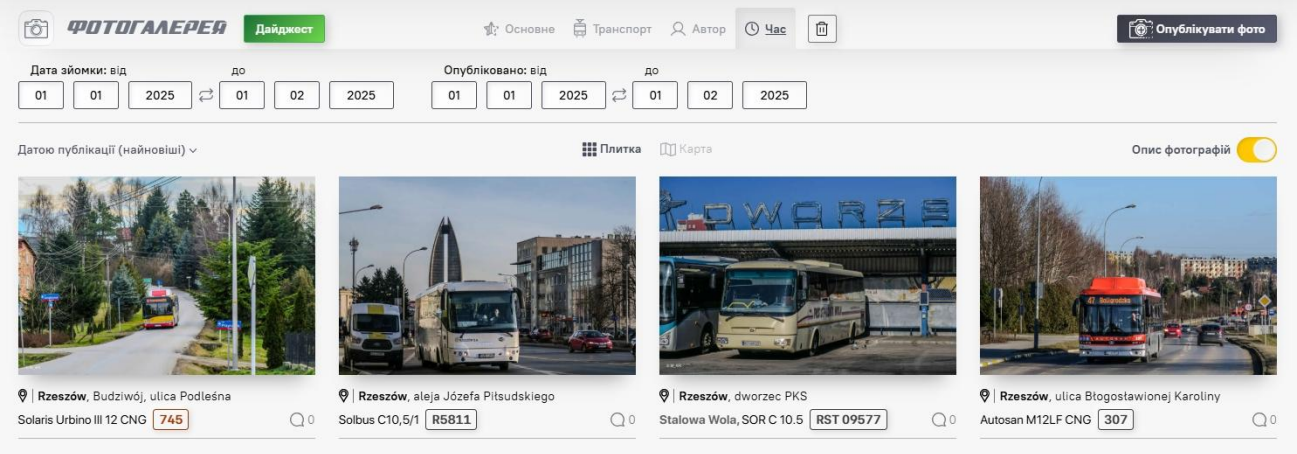


Рисунок 1.9 – Фільтрація фотографій за часовими характеристиками

Окрім цього, всі категорії фільтрів можна поєднувати і таким чином звужувати коло пошуку фотографій, як на рис. 1.12:

Рисунок 1.10 – Комбінований пошук фотографій: застосовано фільтрацію за основними, авторськими та часовими характеристиками і таким чином, здійснено пошук фотографій, знятих в першій половині 2025 року автором Romann, де ТЗ належить Львову, є тролейбусом, який перебуває на 25 маршруті

Фільтрація коментарів надає змогу здійснювати пошук коментарів в межах конкретної територіальної одиниці (міста, області, країни), в межах фотографій, зроблених конкретним автором та коментарів, залишених конкретних автором.

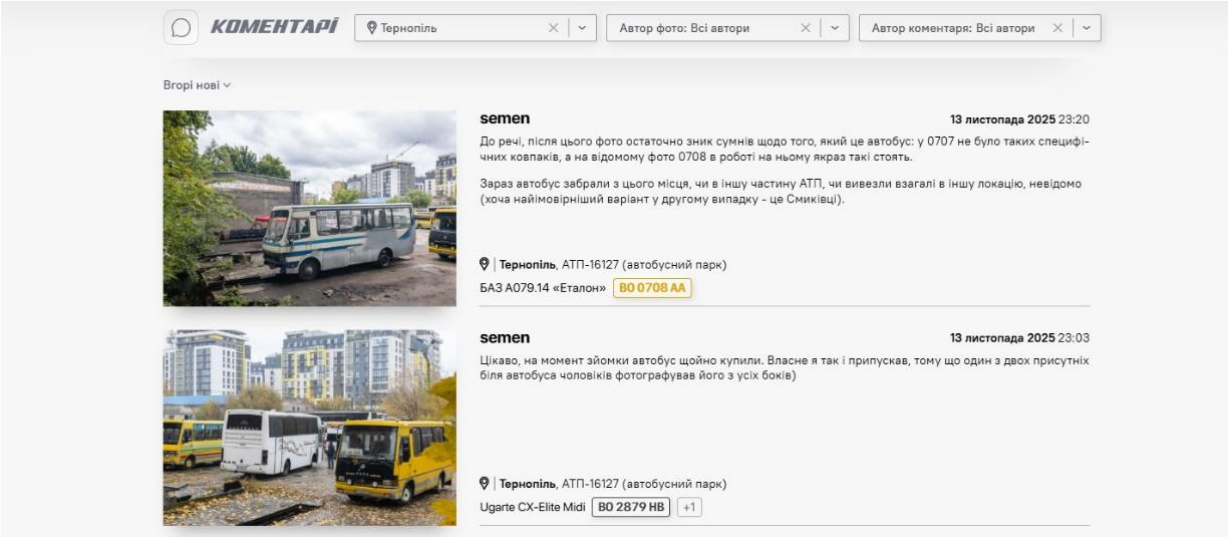


Рисунок 1.11 – Фільтрація коментарів за регіоном

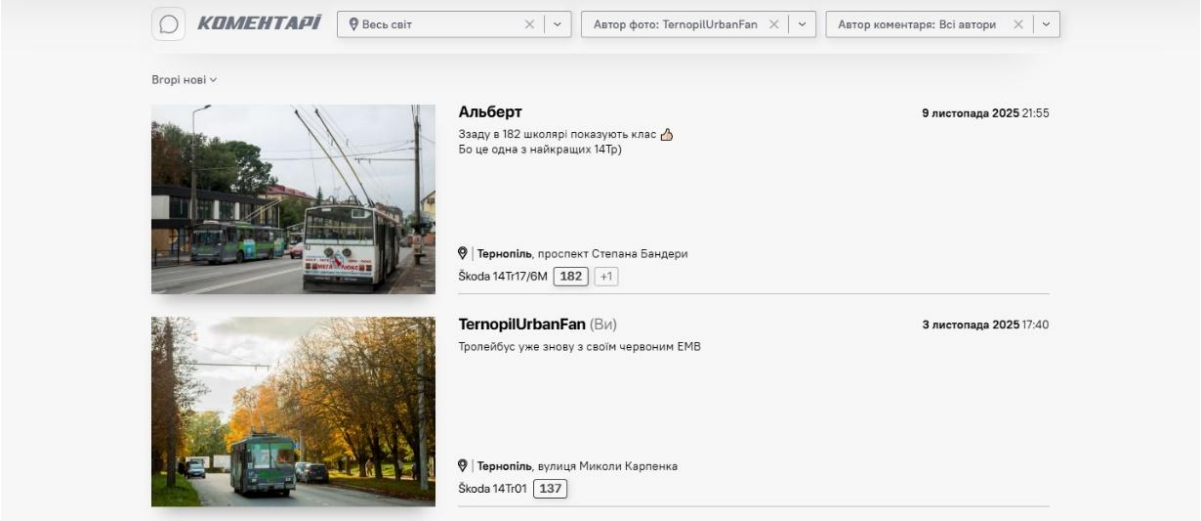


Рисунок 1.12 – Фільтрація коментарів за автором фото, під яким ці коментарі були опубліковані

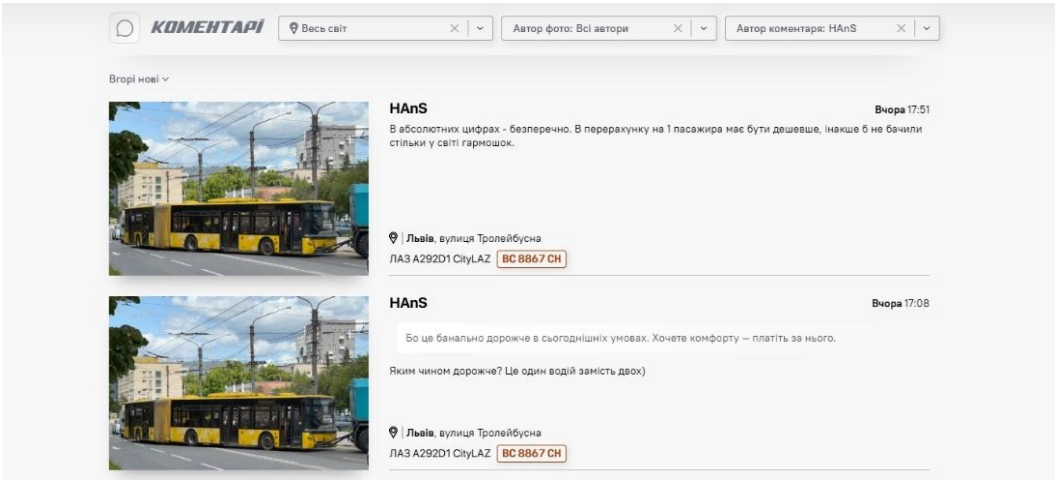


Рисунок 1.13 – Фільтрація коментарів за їхнім автором

Також можна застосувати усі фільтри одразу, як на рис. 1.14:

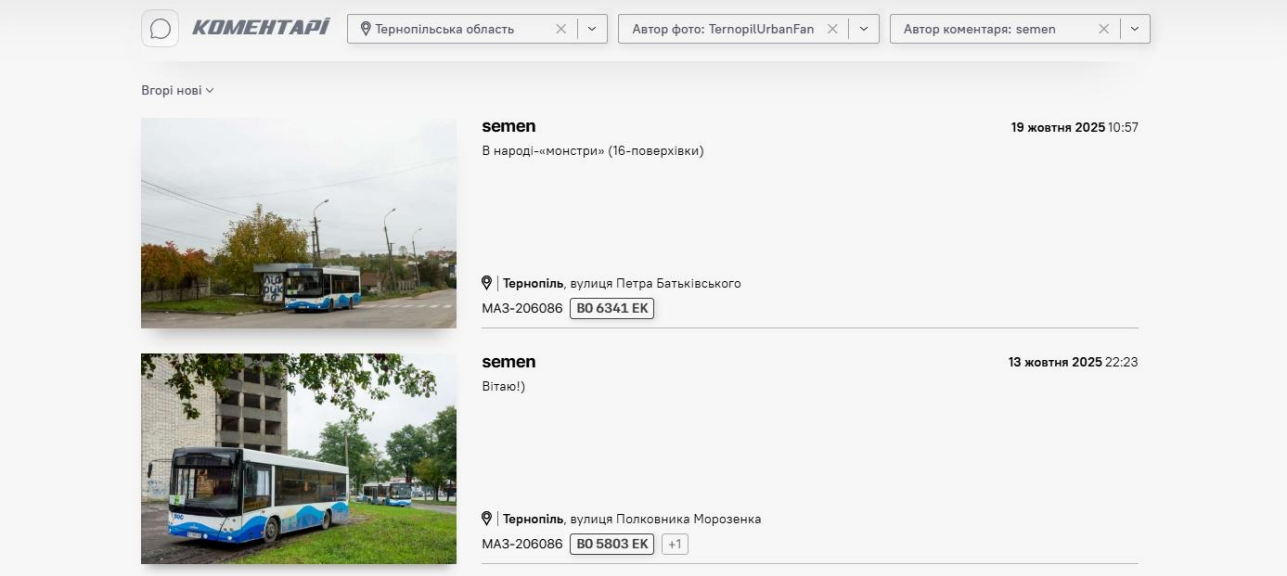


Рисунок 1.14 – Комбінована фільтрація коментарів

Також є можливість фільтрувати дописи, які в AllTransUA поділяються в свою чергу на новини та блоги, до яких найчастіше відносяться дослідження, цікаві факти, історію розвитку громадського транспорту. Фільтрацію дописів можна здійснювати за категоріями, регіоном та автором допису, як на рис. 1.15 – 1.17.

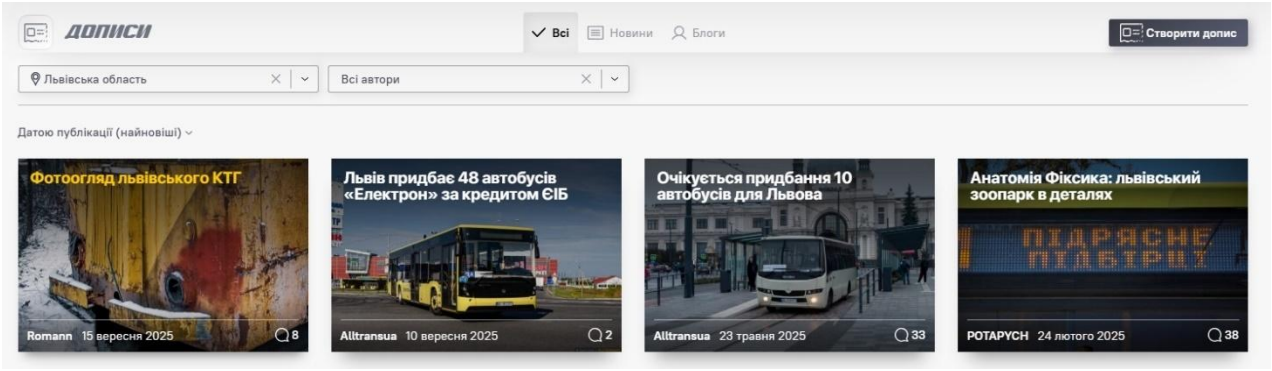


Рисунок 1.15 – Фільтрація дописів за регіоном

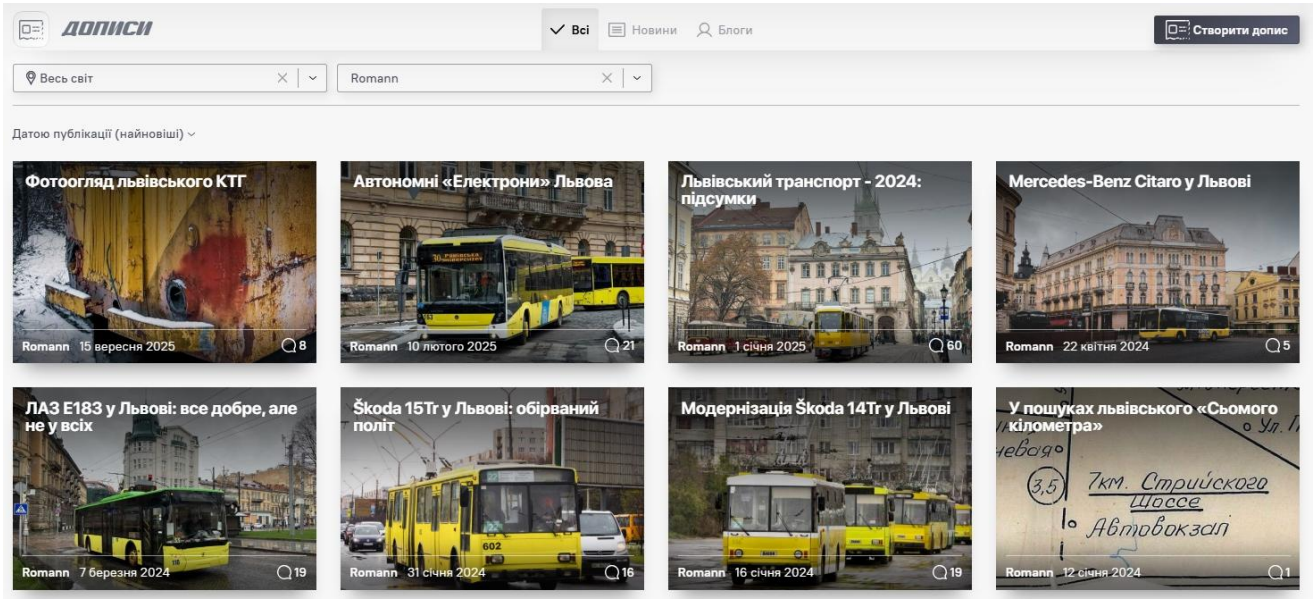


Рисунок 1.16 – Фільтрація дописів за автором публікації

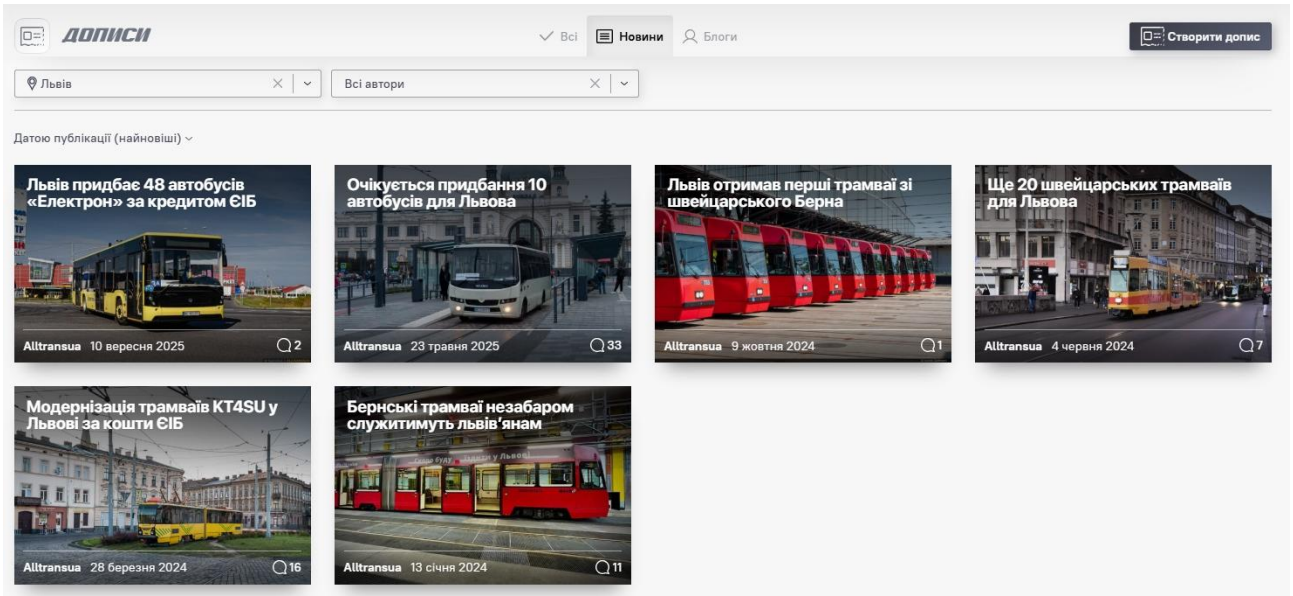


Рисунок 1.17 – Фільтрація дописів за категорією

Як і у випадках з фотографіями та коментарями, можна застосувати комбінований пошук, як на рисунку 1.18:

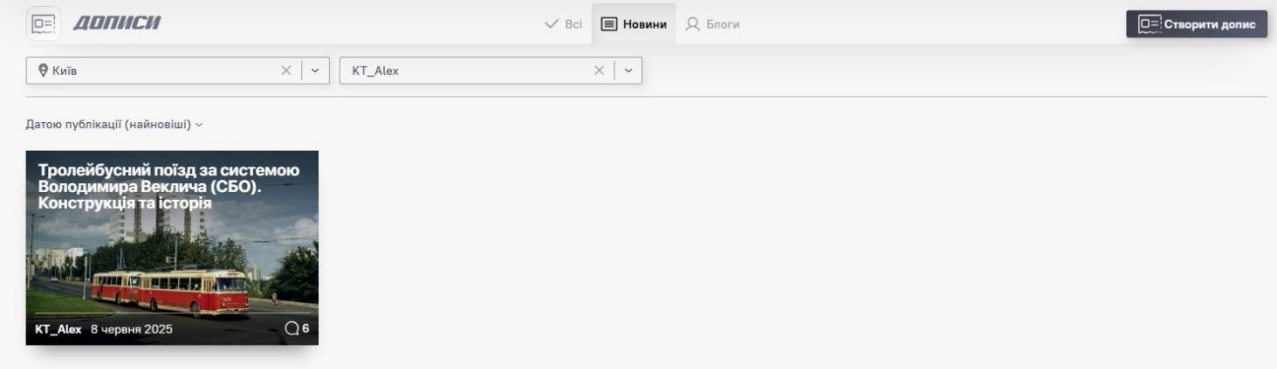
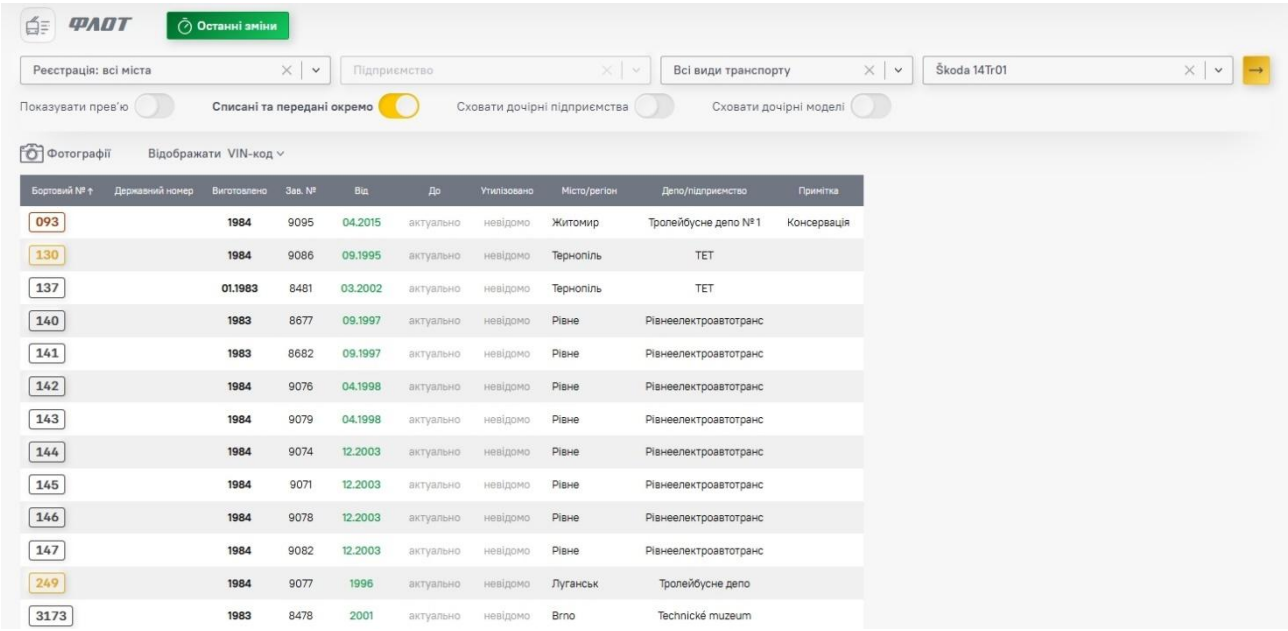


Рисунок 1.18 – Комбінована фільтрація дописів (хоча за характеристикою допис в більшій мірі відповідає категорії “Блоги”)

Останнім розділом, де може відбуватися фільтрація, є перегляд флоту рухомого складу громадського транспорту

Фільтрацію флоту (рухомого складу ГТ) можна здійснювати за наступними параметрами – область/місто, підприємство, види транспорту та модель, як вказано на рис. 1.19 – 1.22:



Бортовий №	Державний номер	Виготовлено	Зав. №	Від	До	Утилізовано	Місто/регіон	Депо/підприємство	Примітка
093		1984	9095	04.2015	актуально	невідомо	Житомир	Тролейбусне депо №1	Консервація
130		1984	9086	09.1995	актуально	невідомо	Тернопіль	ТЕТ	
137		01.1983	8481	03.2002	актуально	невідомо	Тернопіль	ТЕТ	
140		1983	8677	09.1997	актуально	невідомо	Рівне	Рівнеелектроавтотранс	
141		1983	8682	09.1997	актуально	невідомо	Рівне	Рівнеелектроавтотранс	
142		1984	9076	04.1998	актуально	невідомо	Рівне	Рівнеелектроавтотранс	
143		1984	9079	04.1998	актуально	невідомо	Рівне	Рівнеелектроавтотранс	
144		1984	9074	12.2003	актуально	невідомо	Рівне	Рівнеелектроавтотранс	
145		1984	9071	12.2003	актуально	невідомо	Рівне	Рівнеелектроавтотранс	
146		1984	9078	12.2003	актуально	невідомо	Рівне	Рівнеелектроавтотранс	
147		1984	9082	12.2003	актуально	невідомо	Рівне	Рівнеелектроавтотранс	
249		1984	9077	1996	актуально	невідомо	Луганськ	Тролейбусне депо	
3173		1983	8478	2001	актуально	невідомо	Brno	Technické muzeum	

Рисунок 1.19 – Фільтрація флоту за регіоном

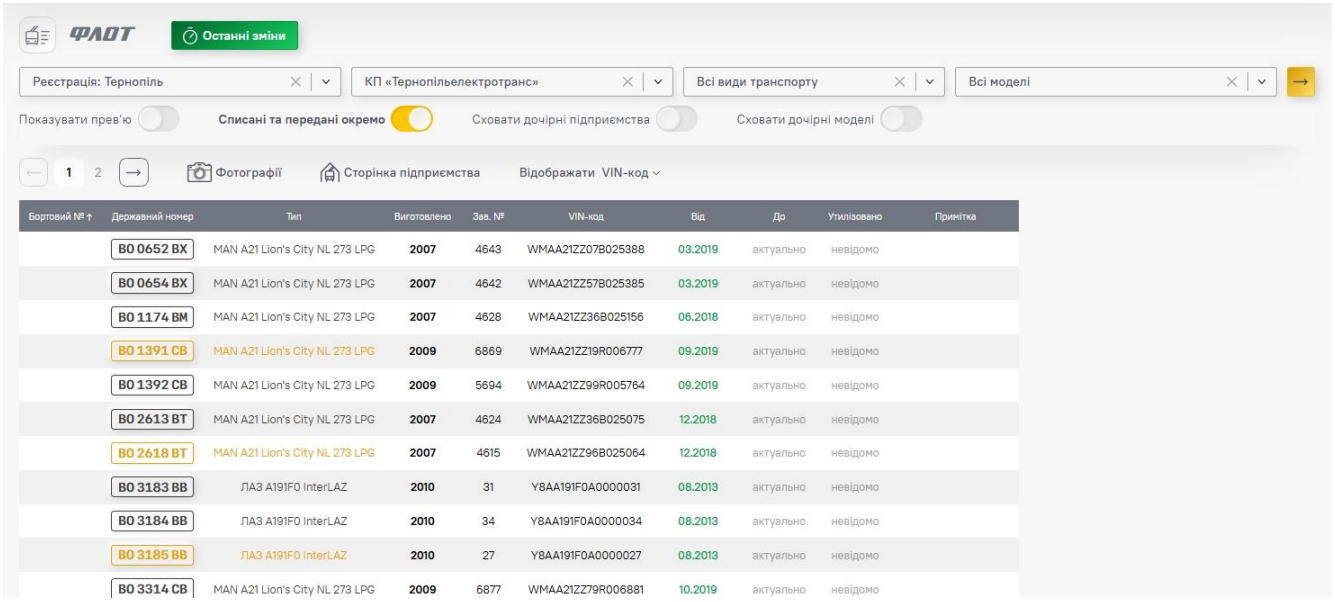


Рисунок 1.20 – Фільтрація флоту за підприємством

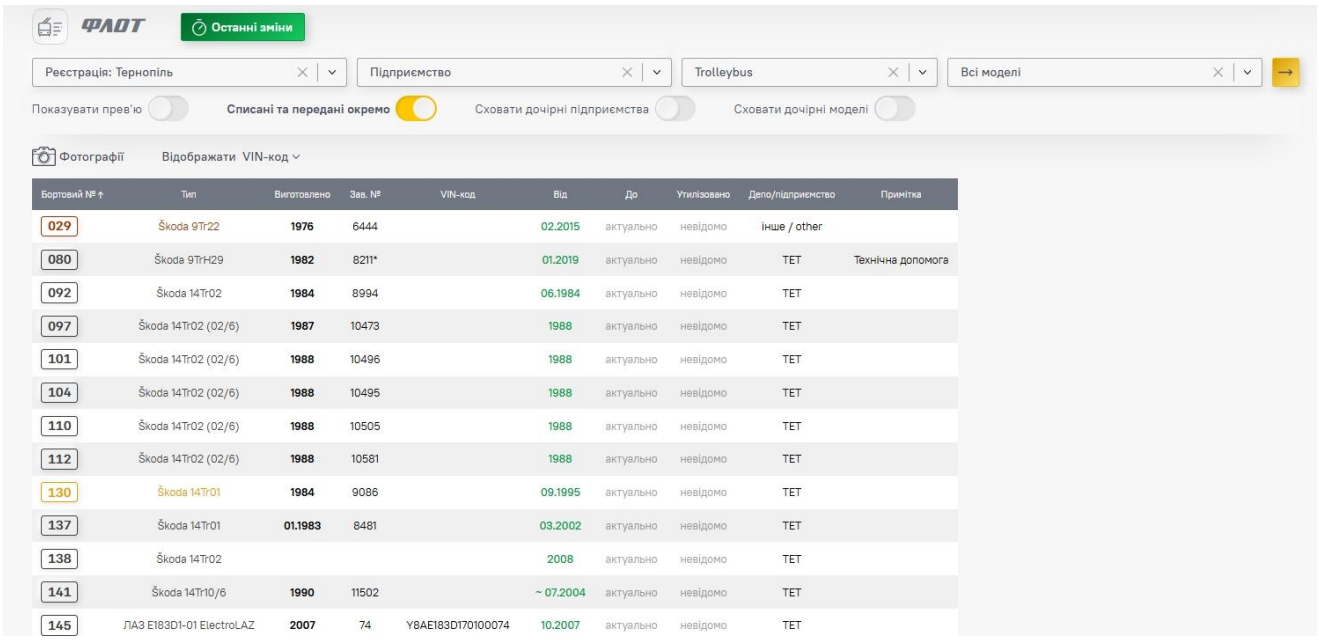


Рисунок 1.21 – Фільтрація флоту за видом транспорту

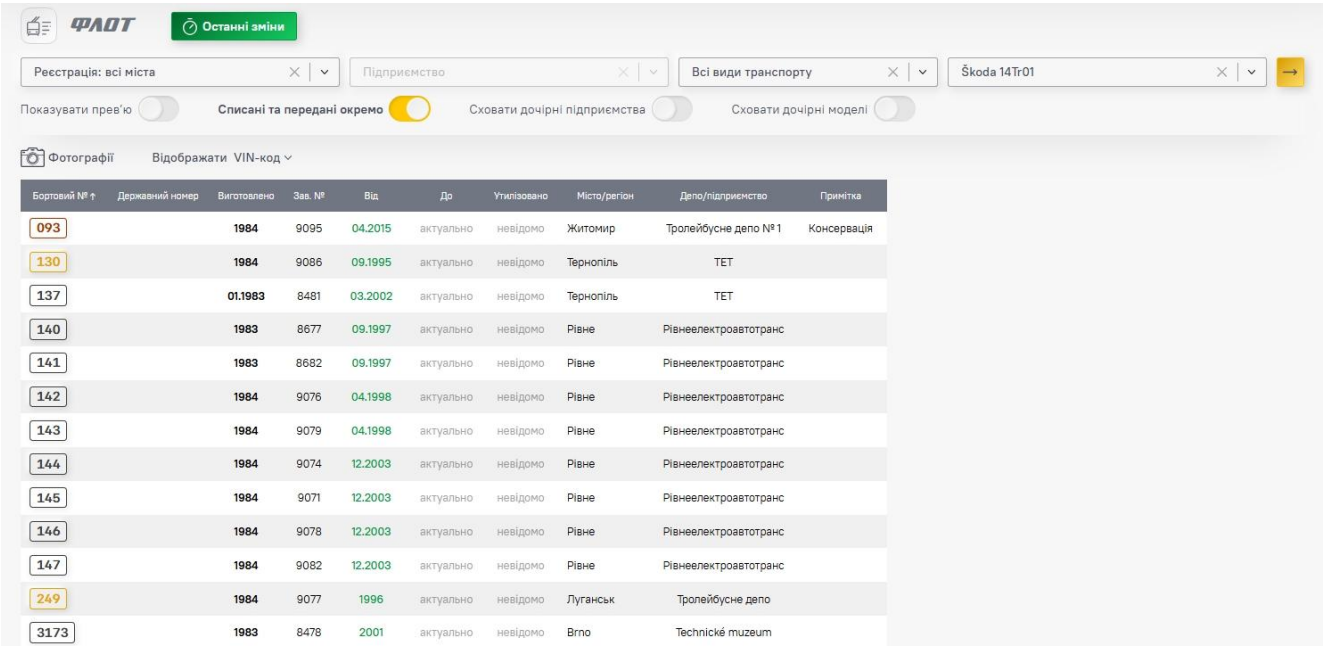


Рисунок 1.22 – Фільтрація флоту за моделлю

Як і у випадках з фотографіями та коментарями, можна застосувати комбінований пошук, як на рисунку 1.23:

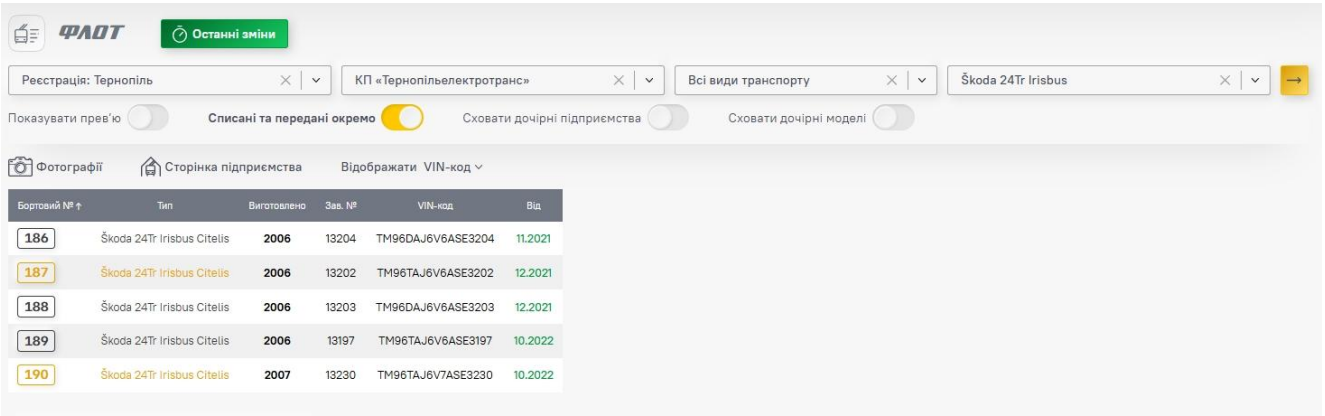


Рисунок 1.23 – Комбінована фільтрація флоту: за містом, підприємством і моделлю

Також варто згадати, що окрім цих інструментів, також існує окремий елемент фільтрації, який не інтегрований в систему перегляду флоту, а саме пошук рухомого складу за державним або бортовим ідентифікаційним номером, як на рисунку 1.24:

Рисунок 1.24 – Пошук флоту за державним або бортовим ідентифікаційним номером як окремий елемент фільтрації РС

1.3 Ієрархія ролей

У рамках функціонування веб-системи передбачено чітко структуровану ієрархію ролей, спрямовану на забезпечення ефективного управління контентом, базою даних (надалі – БД) та процесами модерації. Розмежування повноважень дозволяє мінімізувати ризики помилок, уникати перевантаження окремих ланок і забезпечувати контроль якості інформації. Нижче наведено опис основних категорій користувачів та їхніх функціональних повноважень.

Звичайні користувачі є базовою категорією учасників системи та не володіють жодними адміністративними чи модераційними повноваженнями. Їхні можливості обмежуються переглядом інформації, додаванням фотографій та коментарів, а також редагуванням власного профілю (окрім зміни назви облікового запису, яку мають право здійснювати лише адміністратори).

Важливою складовою актуалізації інформації на транспортному додатку AllTransUA є локальні редактори. Локальні редактори поділяються на вказані ланки:

- локальні редактори підприємства – відповідають за внесення змін до БД у межах конкретного підприємства. Вони можуть редагувати інформацію щодо характеристик підприємства, його структурних елементів, обладнання чи інших даних, доступних у системі. Дана роль призначається лише за умови, що користувач компетентний у відповідній сфері та може підтримувати актуальність інформації.

- локальні редактори міста – відповідають за БД по всьому місту. Їхня діяльність охоплює всі підприємства та об’єкти, якщо для конкретного підприємства не призначено локального редактора підприємства, який спеціалізується на відповідній тематиці. У разі відсутності такого спеціаліста локальний редактор міста забезпечує актуальність даних на рівні міста.

- локальні редактори субрегіональних територіальних одиниць – відповідають за внесення правок в БД на рівні адміністративно-територіальних одиниць субдержавного рівня: областей, республік, автономних округів, повітів, гмін, воєводств (Польща), федеративних земель (Німеччина), штатів, провінцій (США) тощо. Їхні повноваження охоплюють редагування бази даних у межах усієї відповідної території, якщо в окремих містах цього субрегіону відсутні локальні редактори нижчих рівнів. Таким чином, ця категорія забезпечує заповнення прогалин у редакторській структурі та БД на рівні певної області.

- локальні редактори країни – відповідають за повноцінне редагування всієї БД у межах однієї держави. Їхні функції активуються в тих випадках, коли на рівні субрегіонів чи міст відсутні відповідні редактори. Вони забезпечують цілісність і актуальність національного сегмента даних та можуть виконувати загальний контроль якості інформації, а також забезпечують заповнення прогалин у редакторському колективі та БД на рівні певної країни

- загальні локальні редактори – найвища ланка редакторів, яким надано можливість редагувати БД на глобальному рівні — по всьому світу. Їхня роль важлива у випадках, коли в окремих країнах або регіонах немає редакторів

нижчих ланок. Загальні локальні редактори забезпечують підтримку повноти та послідовності світової бази даних.

Для забезпечення упорядкованості фотогалереї від постороннього контенту (переважно недостатньо якісного) та контенту, що не відповідає тематиці транспортного додатка AllTransUA (включно і контенту, що протирічить законодавству України та/або має певний гриф секретності), для підтримки здорової взаємодії користувачів між собою та впорядкованості інформації, що циркулює в форумах, існує особовий склад модераторів, які в свою чергу, поділяються на три різні категорії:

1) фотомодератори – відповідають за перевірку, оцінювання та обробку користувацьких фото. До їхніх повноважень належать:

- схвалення або відхилення завантажених фотографій;

- відправлення фотографій на доопрацювання з поясненням недоліків;

- заміна або видалення фотографій на прохання користувача без зазначення недоліків (якщо цього вимагає сам користувач);

- відновлення видалених зображень у разі потреби.

Ця роль забезпечує якість візуального контенту та попереджує публікацію некоректних чи неприйнятних зображень.

2) модератори коментарів – працюють над коментарями користувачів. Вони здійснюють перевірку коментарів користувачам, що перебувають на премодерації коментарів, та приймають рішення про їхнє схвалення або відхилення. Метою є підтримання культури спілкування та запобігання порушенням правил спільноти.

3) модератори форумів – здійснюють контроль за змістом дописів у тематичних обговореннях, мають право редагувати вміст повідомлень, видаляти їх у випадках порушення правил або неправдивості, а також підтримувати порядок та структурованість дискусій.

4) адміністратори – найвища ланка управління сайтом. Вони володіють найширшим спектром повноважень, включно з:

- блокуванням користувачів або переведенням їх у режим read-only;

- видаленням коментарів;

- направленням користувачів на премодерацію фотографій або коментарів;

- призначенням фотомодераторів та локальних редакторів бази даних різних рівнів;

- редагуванням текстових описів до фотографій;

- заміною або видаленням фото на прохання користувачів та відновленням видалених зображень.

Адміністратори забезпечують повне операційне управління системою та вирішують складні або спірні ситуації.

1.4 Система модерації контенту та скарг

Система модерації транспортного порталу AllTransUA є комплексним механізмом контролю якості контенту, який забезпечує перевірку достовірності, коректності та відповідності матеріалів правилам ресурсу. Її основним завданням є підтримання високого рівня інформаційної культури, недопущення поширення некоректних або неправдивих даних, а також забезпечення довіри користувачів до опублікованих матеріалів.

До складу системи модерації входять три ключові підсистеми: система скарг, механізм постмодерації та система премодерації. Кожна з них виконує власні функції та активується за різних умов.

Система скарг дає змогу користувачам повідомляти про недоліки опублікованих матеріалів та сприяє залученню спільноти до підтримки якості контенту. Скарги поділяються на кілька типів залежно від характеру проблеми, як вказано на рис. 1.25:

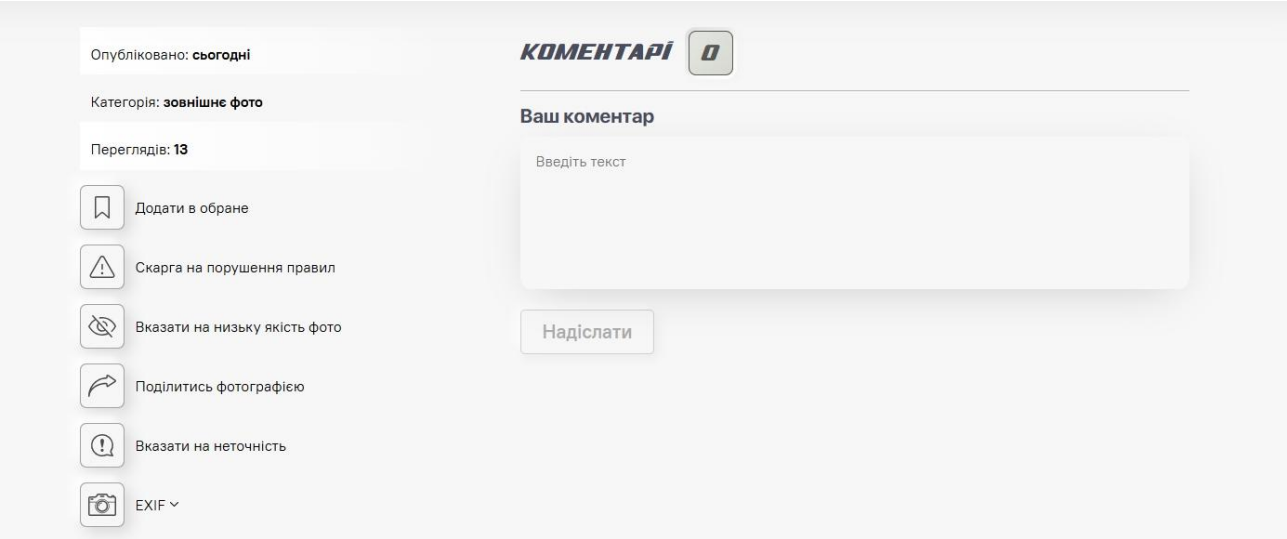


Рисунок 1.25 – Система скарг: скарга на порушення правил, повідомлення про низьку якість фото, вказання на неточність

А) вказання на порушення правил – застосовується, якщо фотографія безпосередньо порушує правила платформи або норми етики (якщо зображення містить нецензурну лексику, образи на адресу користувача / групи користувачів), конфіденційну або заборонену до поширення інформацію, матеріали, що порушують авторські права), або ж коли фотографія не відповідає тематичній спрямованості порталу.

Б) вказання на низьку якість фото – може бути подана лише впродовж перших трьох днів після публікації фотографії. Після її надходження модератори мають право перевести фото на модерацію та провести перевірку технічної якості фото на наявність недоліків (завал горизонту, невдалі кольори, викривлені пропорції тощо) і прийняти відповідне рішення стосовно фото: прийняти, відправити на доопрацювання або відхилити

В) вказання на неточність фото – подається у випадку неправильно зазначених даних: помилки в описі, некоректно прив’язаний профіль транспортного засобу, невірно обраний тип фото, хибно вказаний маршрут або інші неточності, які можуть вводити користувачів в оману, проте в такому випадку скарга адресується власнику фото, а не фотомодераторам

Система скарг дозволяє оперативно виявляти помилки та підвищувати якість як фотоматеріалів, так і супровідної інформації.

Постмодерація є механізмом перевірки фотографій після їх публікації. Це означає, що зображення одразу стає доступним для перегляду іншими користувачами, але може бути додатково перевірене фотомодераторами за наявності підозр на недоліки або після надходження відповідних скарг.

Постмодерація дозволяє збалансувати швидкість публікації контенту з необхідністю контролю якості, адже дає змогу втручатися лише тоді, коли виникає обґрунтована потреба. Одним словом, коли користувач перебуває на постмодерації (не перебуває на премодерації), то має право прямої публікації фотоконтенту та коментарів, як вказано на рисунку 1.26:

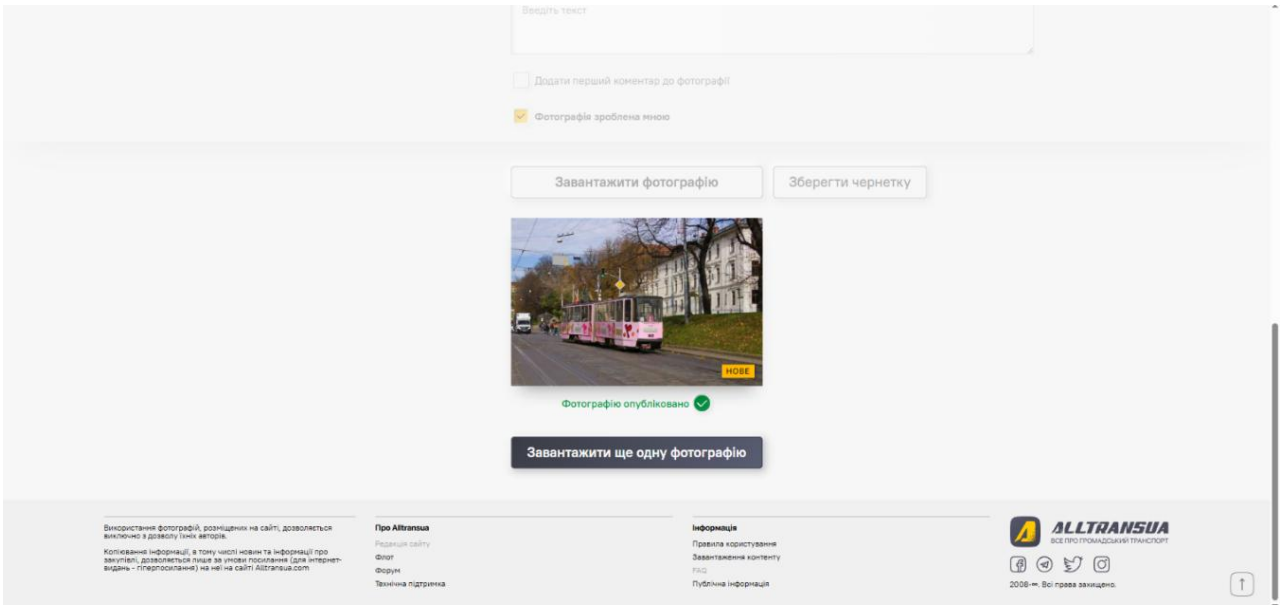


Рисунок 1.26 – Публікація фотоматеріалів на умовах постмодерації

Премодерація передбачає обов’язкову перевірку фотографії до моменту її публікації. Після завантаження зображення переходить у чергу на розгляд фотомодераторів, які приймають одне з трьох рішень, вказаних на рис. 1.27:

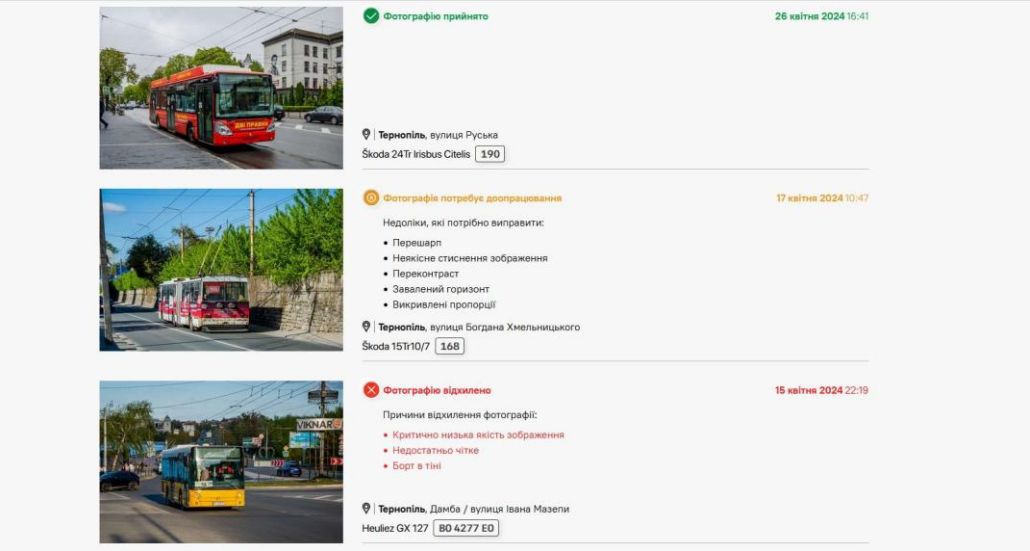


Рисунок 1.27 – Три різні результати премодерації фотографій

- схвалити фото – у такому разі фото публікується;

- відправити на доопрацювання – користувачу надаються вказівки щодо виправлення недоліків;

- відхилити фото – якщо зображення грубо порушує правила або не підлягає якісному виправленню.

Премодерація є важливою складовою для контролю користувачів, які систематично публікували фотоматеріали недостатньої якості, поки перебували в стані постмодерації фото.

Коли користувач перебуває на премодерації, при публікації фотоматеріалів з’являється сповіщення, що фотографія була поставлена в чергу на модерацію, як на рисунку 1.28:

Окрім цього, є випадки, на які премодерація поширюється на більшість користувачів – йдеться про можливість публікації неавторського контенту, окрім цього, там необхідно вказати тип ліцензії, першоавтора (якщо першоавтор не бажає розкривати своєї особи, автора потрібно все одно вказати, проте як “автор анонімний”), як вказано на рис. 1.29 та рис. 1.30.

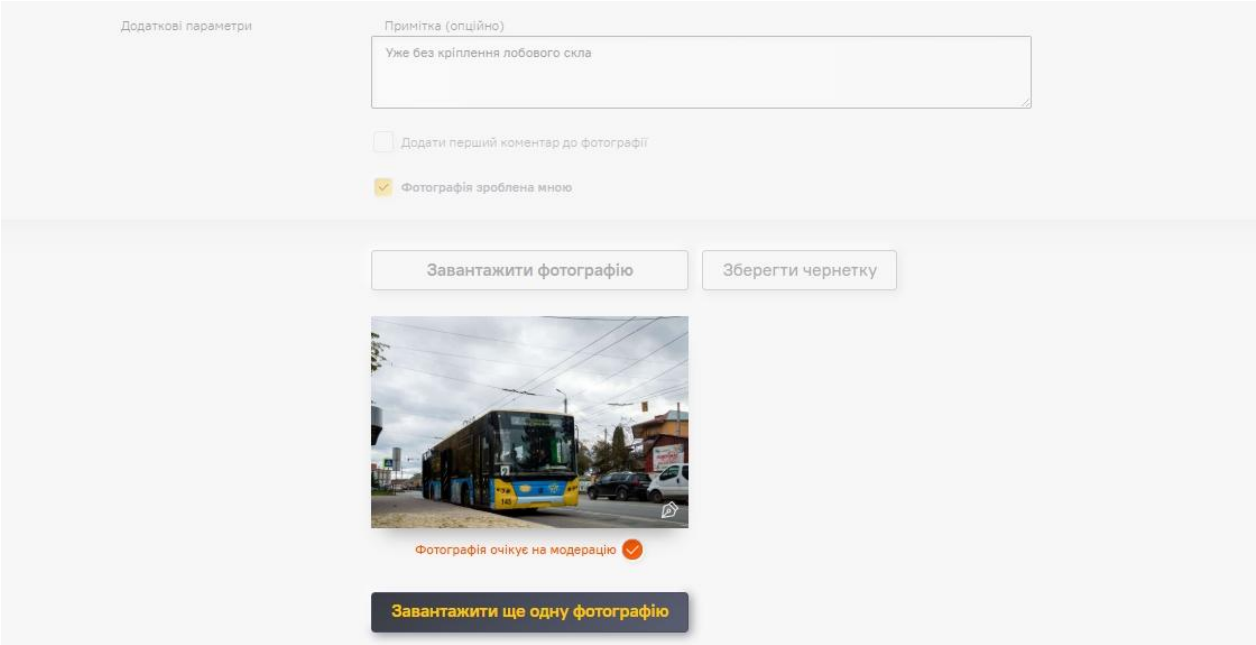


Рисунок 1.28 – Публікація фотоматеріалів на умовах премодерації

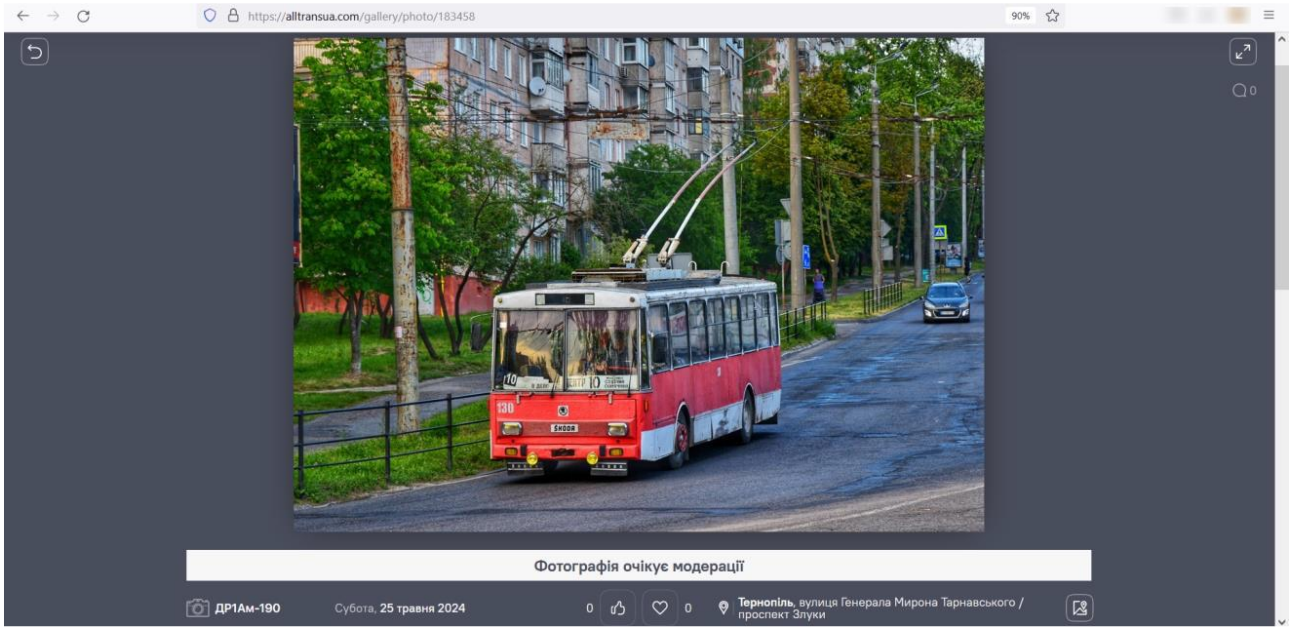


Рисунок 1.29 – Публікація фотоматеріалів на умовах премодерації, що поширюється на більшість випадків публікації неавторського контенту [1]

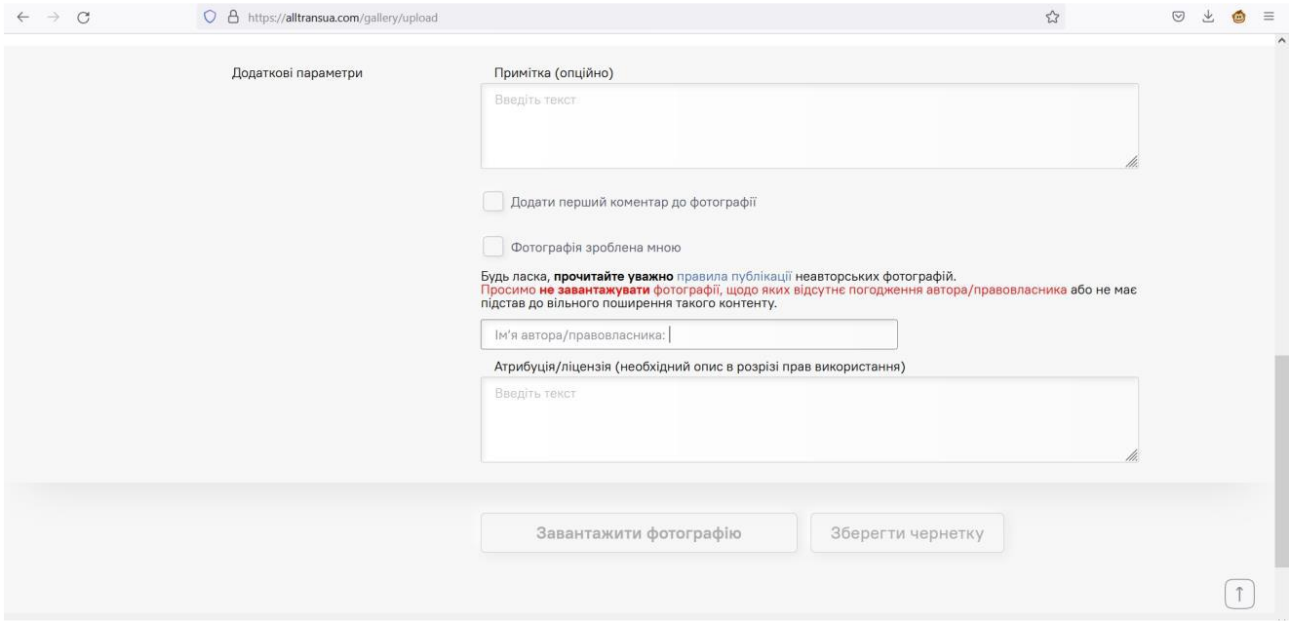


Рисунок 1.30 – Політика щодо неавторських фотографій [1]

Важливо зазначити, що модерація стосується не лише фотографій, а й коментарів – якщо користувач грубо порушує правила етики, то йому загрожує принаймні модерація коментарів – коментар публікується не одразу, а проходить модерацію відповідними особами, а саме модераторами коментарів, які вирішують, прийняти коментар чи відхилити. Рішення про переведення користувачів на премодерацію фотографій та коментарів приймають виняткова адміністратори сайту AllTransUA.

1.5 Журналювання даних

Журналювання даних є одним із ключових механізмів забезпечення прозорості, відтворюваності та контролю цілісності інформації в інформаційних системах. Цей процес передбачає систематичний запис змін, що відбуваються з даними, з метою подальшого аналізу, аудиту, відстеження історії правок та виявлення потенційних порушень чи неточностей. У контексті транспортного порталу AllTransUA журналювання відіграє важливу роль у підтриманні достовірності інформації про транспортні засоби (ТЗ), забезпечуючи можливість простежити будь-які зміни, внесені користувачами, локальними редакторами чи адміністраторами.

На даному етапі розвитку системи на порталі реалізовано журналювання лише одного типу даних – змін у базі даних транспортних засобів. Кожен запис у журналі містить обмежений, але достатній для аудиту набір метаданих. Це дозволяє фіксувати критично важливі атрибути ТЗ, що зазнали редагування, а також визначати, хто саме та коли вніс ці зміни. Такий підхід забезпечує базовий рівень контролю над історією модифікацій та підтримує принципи відповідальності суб’єктів, що беруть участь у наповненні та коригуванні даних.

До переліку параметрів, що фіксуються у журналі змін, входять:

- бортовий номер транспортного засобу – ключовий ідентифікатор, який найчастіше підлягає оновленню у випадках переведення ТЗ між підрозділами чи зміни внутрішньої нумерації;

- державний реєстраційний номерний знак – офіційний ідентифікаційний параметр, зміна якого потребує особливого контролю через можливість виникнення помилок або дублювання;

- тип транспорту – хоча в таблиці правок цей параметр явно не відображений, система передбачає його врахування у структурі журналу, що є важливим для коректної категоризації ТЗ;

- модель транспортного засобу – характеристика, зміна якої може впливати на класифікацію та пошук об’єктів у базі даних;

- місто експлуатації транспортного засобу – атрибут, що має значення для територіального розподілу редакторських повноважень та формування достовірної карти транспорту;

- підприємство, на балансі якого перебуває ТЗ – параметр, що прямо залежить від структури місцевих транспортних операторів та вимог до точності інформації;

- дата внесення правки – визначає час здійснення зміни та дозволяє аналізувати динаміку оновлень;

- автор правки – ідентифікація користувача, який здійснив зміну, що забезпечує механізм відповідальності та можливість зворотного зв’язку.

Користувачі на власний розсуд можуть здійснювати фільтрацію правок записів БД за наступними параметрами, зокрема: весь світ / країна / область /

місто, підприємство, тип транспорту та модель транспорту, як на рисунках 1.31 – 1.34:

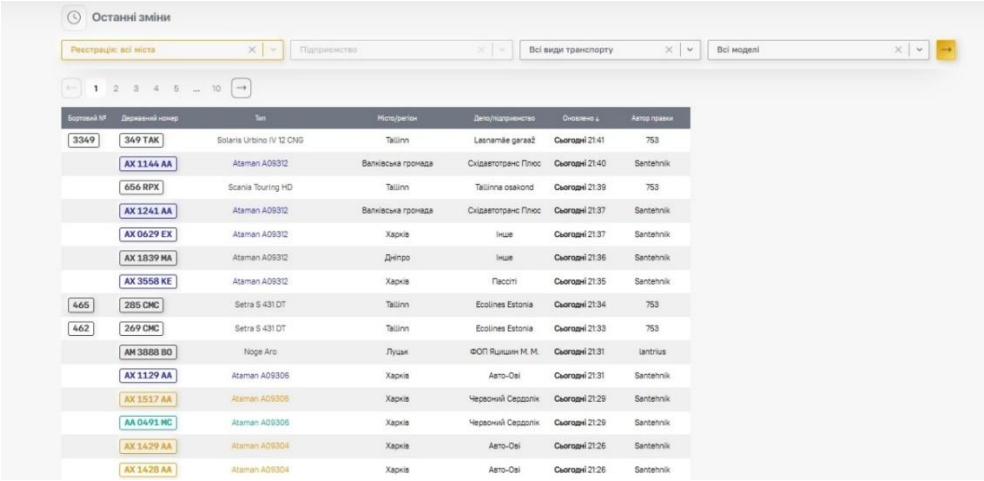


Рисунок 1.31 – Перегляд журналу правок БД на рівні всього світу

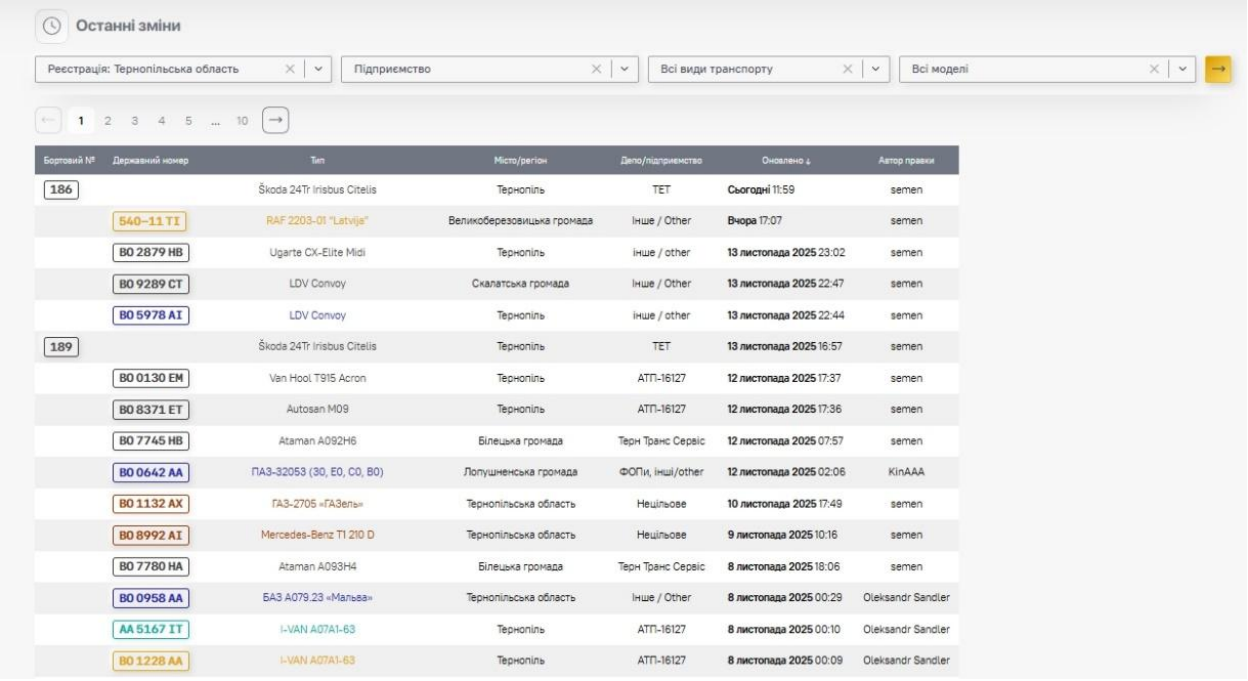


Рисунок 1.32 – Перегляд журналу правок БД на рівні області

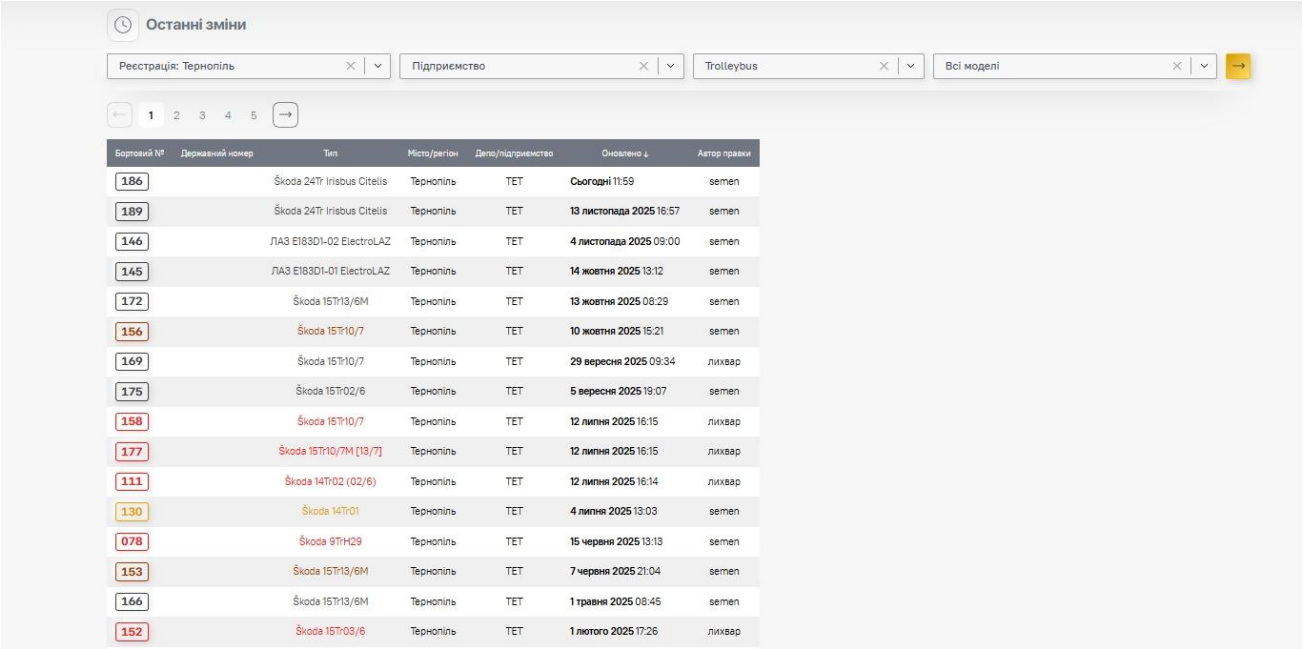


Рисунок 1.33 – Перегляд журналу правок БД на рівні підприємства

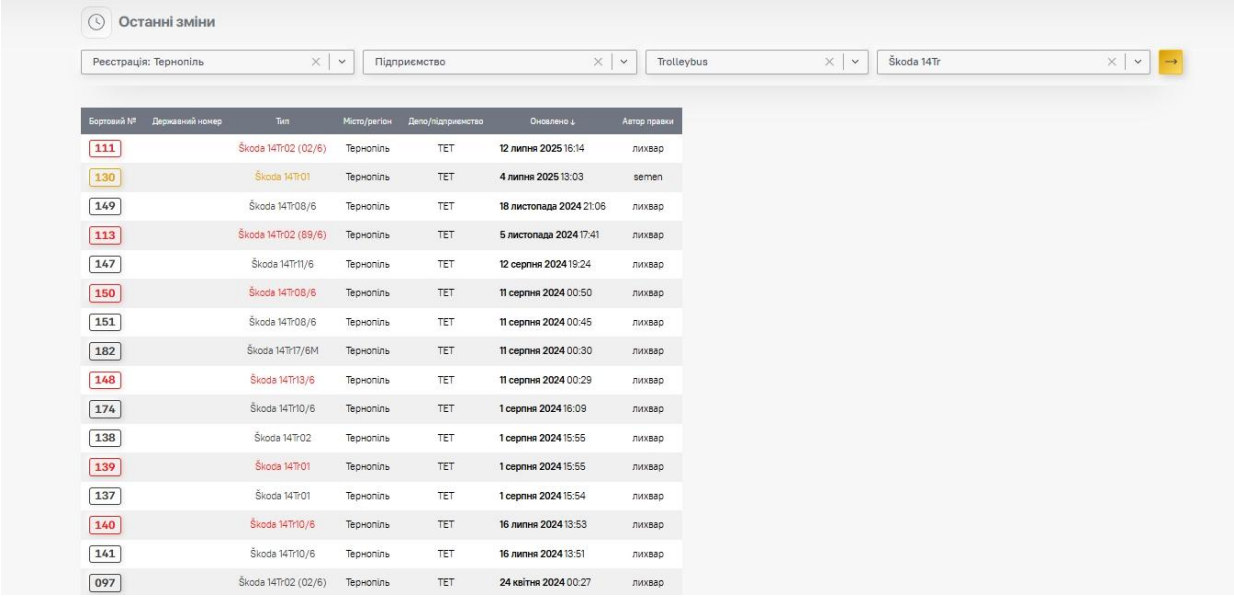


Рисунок 1.34 – Перегляд журналу правок БД з застосуванням усіх параметрів пошуку

Журналювання таких даних дозволяє підтримувати точність та актуальність БД транспортних засобів, а також створює необхідну основу для подальшого вдосконалення системи контролю. Попри те, що перелік фіксованих атрибутів є обмеженим, він забезпечує фундаментальні можливості аудиту та дозволяє проводити аналіз змін, що відбуваються у базі даних порталу.

Варто зазначити, що коли користувач додає фото нового ТЗ, відсутнього в БД, йому пропонується можливість додати новий запис в БД і створити новий ТЗ, таким чином, БД можуть правити і пересічні користувачі, що може створювати ряд зайвої роботи локальним редакторам.

Проте система журналювання потребує доопрацювання – оскільки журналювання змін привілеїв користувачів не проводиться, це відкриває шлях адміністраторам до ряду зловживань, зокрема прихованого підвищення привілеїв користувачам за принципом “свій, значить можна” або необгрунтованого позбавлення посад.

1.6 Система реєстрації та входу

Система реєстрації та автентифікації користувачів у веб-порталі AllTransUA забезпечує базовий рівень контролю доступу до персоналізованих функцій сайту, включаючи можливість публікувати фотографії, залишати коментарі, редагувати дані транспортних засобів у межах наданих повноважень та взаємодіяти з іншими користувачами. Реалізований механізм авторизації є необхідною частиною роботи порталу, оскільки дозволяє ідентифікувати суб’єктів, що здійснюють дії в системі, а також забезпечує виконання принципу відповідальності за внесені зміни.

Процес входу передбачає використання двох основних параметрів — імені користувача та пароля, що є стандартною практикою для класичних веб-систем автентифікації. У разі втрати доступу користувачеві доступна опція «Забули пароль?», яка дозволяє відновити пароль шляхом підтвердження електронної адреси, як зображено на рис. 1.35 – 1.36:

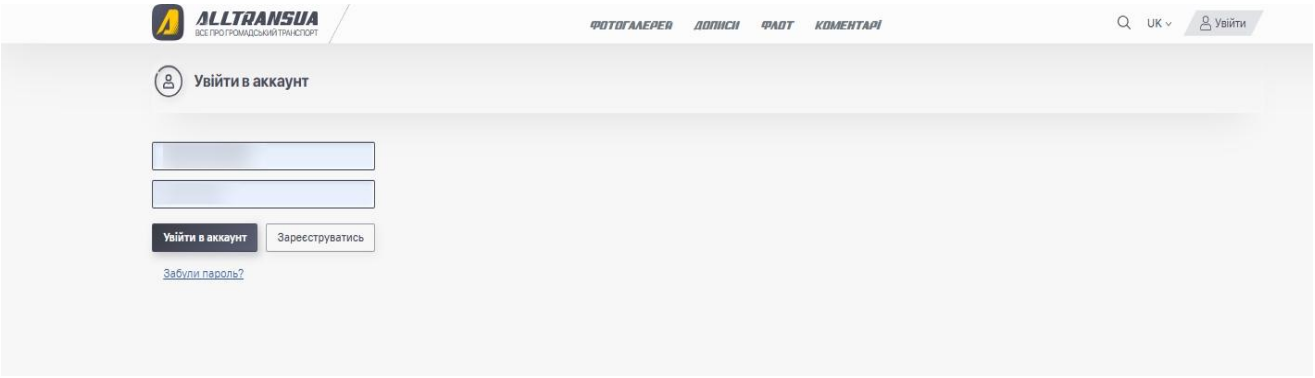


Рисунок 1.35 – Вхід в транспортний додаток AllTransUA, що складається лише з двох компонентів: логін / ім’я акаунта та пароль

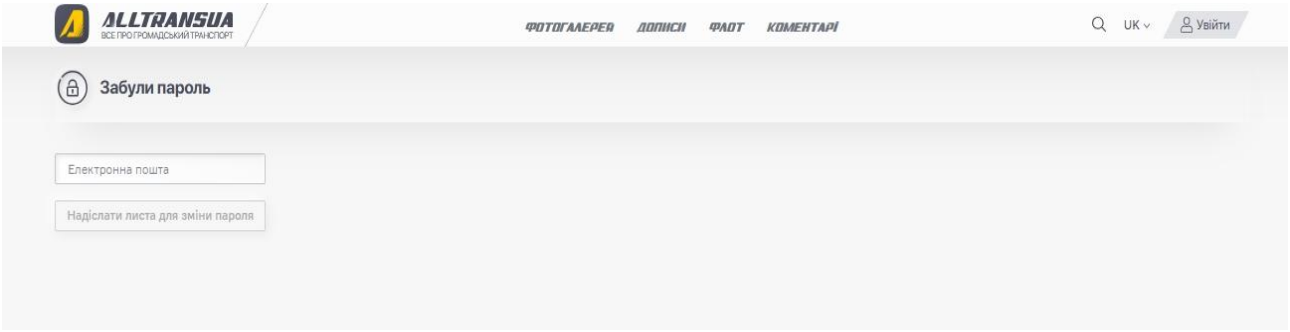


Рисунок 1.36 – Можливість відновлення пароля до акаунта в транспортному додатку AllTransUA

Реєстрація в системі вимагає введення таких даних, як вказано на рис. 1.37:

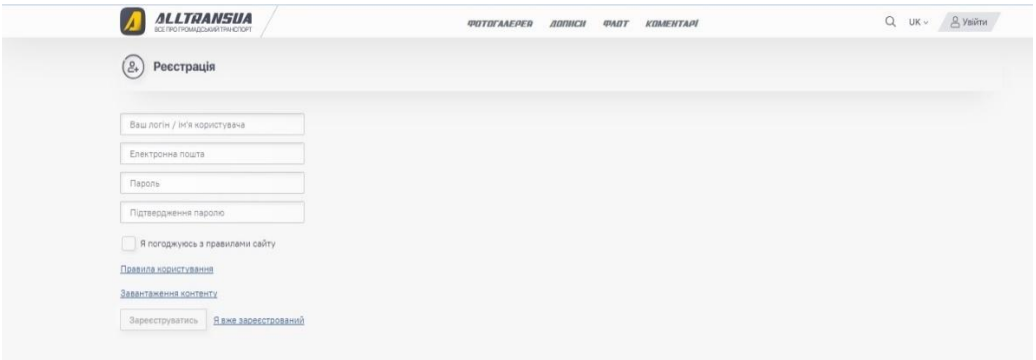


Рисунок 1.37 – Система реєстрації нового акаунта в транспортному додатку AllTransUA

- ім’я або логін, що надалі використовуватиметься для входу;

- електронна пошта, яка виконує роль ідентифікатора облікового запису та засобу комунікації;

- пароль;

- підтвердження пароля для запобігання помилкам при введенні.

Система встановлює обмеження: на одну електронну адресу може бути зареєстровано лише один обліковий запис. Це дозволяє уникнути дублювання облікових записів і спрощує керування користувацькими профілями. Проте на сайті зафіксовані випадки, коли одна особа має два акаунти, що ще більше загострює потребу в багатофакторній автентифікації.

Варто зазначити, що на даний момент у системі відсутня багатофакторна автентифікація (БФА), зокрема такі сучасні методи, як вхід за відбитком пальця або розпізнаванням обличчя. Це може розглядатися як джерело ризику зламу облікових записів, адже паролі зараз є доволі легкою для зламу ціллю, надає змогу обходити блокування акаунту шляхом створення нових облікових записів з прив’язкою до іншої електронної пошти, а також розглядається як потенційний напрямок удосконалення безпеки порталу, оскільки багатофакторна автентифікація суттєво підвищує рівень захисту облікових записів від несанкціонованого доступу.

1.7 Канали комунікації AllTransUA

Комунікація між користувачами, модераторами та адміністрацією є важливим компонентом функціонування порталу AllTransUA. Для цього використовуються спеціалізовані канали зв’язку, створені на платформі Telegram, які сприяють ефективному обміну інформацією, підтримці користувачів та підвищенню якості контенту, що публікується на сайті.

Первинний комунікаційний канал, орієнтований на взаємодію з фотографами та ентузіастами міського транспорту, складається з семи тематичних гілок, кожна з яких виконує окрему функцію, як вказано на рис. 1.38:

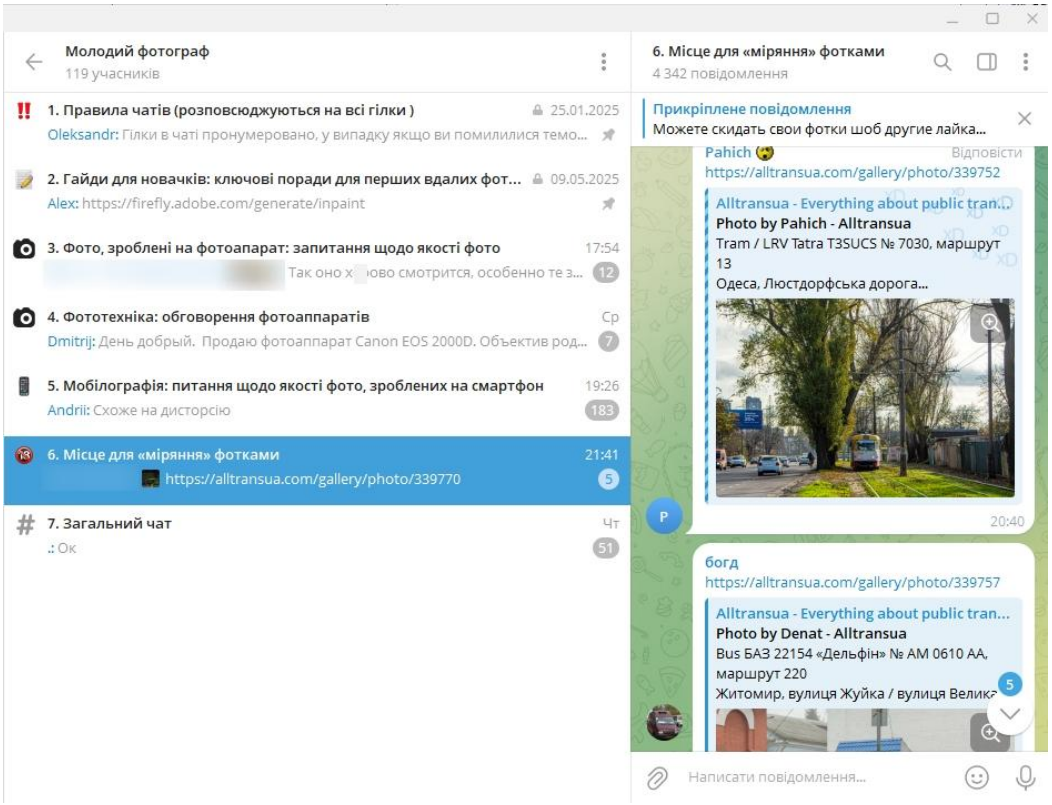


Рисунок 1.38 – Канал комунікації AllTransUA щодо допомоги фотографам з різних питань, включно і початківцям

1. Загальні правила поведінки та етикету в всіх інших гілках чату.
2. Інструкції для новачків у фотографуванні ГТ.
3. Чат з питань оцінки якості фотографій з фотоапаратів фахівцями з навичками фотографування
4. Чат для обговорення та вибору фототехніки.
5. Чат оцінки якості фотографій зі смартфонів фахівцями з навичками фотографування.
6. Гілка для поширення фотографій.
7. Загальний чат, призначений для вільного спілкування на тему транспорту та пов’язаних питань.

Окремо створено спеціальний чат для зв’язку з адміністрацією та модерацією AllTransUA, який виконує роль офіційного каналу технічної підтримки, зображений на рис. 1.39:

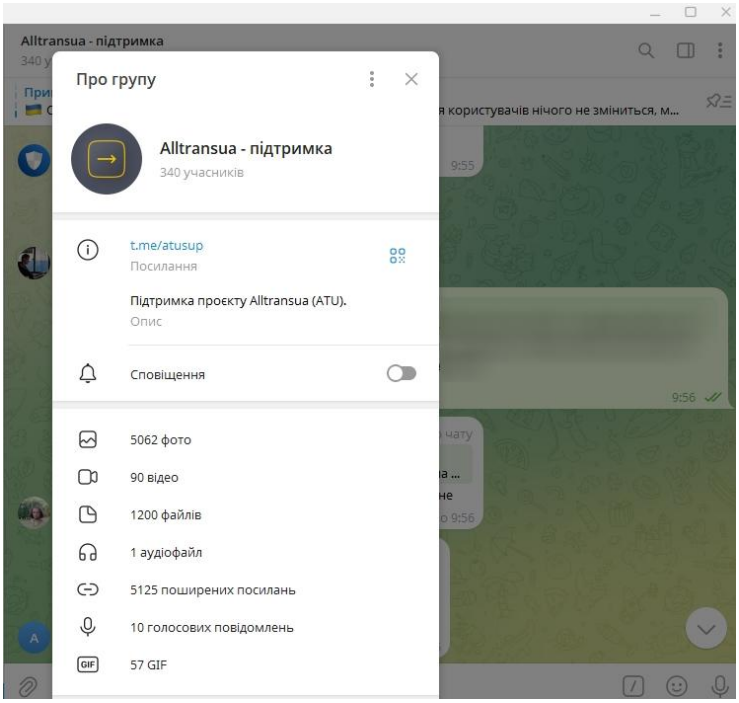


Рисунок 1.39 – Канал з технічної підтримки транспортного додатка AllTransUA

У цьому чаті користувачі можуть звернутися з різними питаннями, зокрема щодо переведення на / зняття з премодерації, рапорти про порушення правил, внести правки в БД, технічні питання щодо роботи додатка, запити на зміну/видалення фотографій.

Таким чином, система комунікації AllTransUA забезпечує структуровану, оперативну та ефективну взаємодію між учасниками спільноти, що сприяє підтриманню високої якості контенту та швидкому реагуванню на проблеми, які виникають під час користування порталом.

1.8 Висновки до першого розділу

Система AllTransUA являє собою багатокомпонентний транспортний веб-портал, робота якого ґрунтується на поєднанні механізмів публікації контенту, модерації, управління користувачами та підтримки актуальності даних про транспортні засоби. Проведений огляд дозволяє зробити висновок, що платформа має розвинену структуру взаємодії між користувачами, редакторами, модераторами та адміністраторами, що забезпечує чіткий розподіл функцій і

відповідальності. Механізми модерації, які включають систему скарг, постмодерацію та премодерацію, створюють необхідні умови для підтримання якості та достовірності контенту, хоча їхня ефективність суттєво залежить від активності та кваліфікації модераторського складу.

Функціонування системи реєстрації та входу характеризується базовою реалізацією засобів автентифікації, що включає використання логіна, електронної пошти та пароля, однак відсутність багатофакторної автентифікації формує потенційні ризики для безпеки облікових записів. Крім того, журналювання змін у базі даних, обмежене лише транспортними характеристиками, не покриває змін у системі ролей користувачів, що знижує рівень прозорості адміністрування.

Важливою складовою функціонування порталу є комунікація між користувачами та адміністрацією, яка реалізується через тематичні Telegram-чати. Даний канал комунікації забезпечує оперативність розв'язання технічних питань, допомагає новачкам засвоїти вимоги до якості фото та сприяє ефективній підтримці спільноти. Загалом система AllTransUA демонструє збалансоване поєднання користувацьких сервісів і модераційних інструментів, проте потребує подальшого розвитку у напрямі підвищення рівня безпеки та розширення можливостей журналювання.

РОЗДІЛ 2 АНАЛІЗ ДЖЕРЕЛ ДОСЛІДЖЕНЬ В ОБРАНИХ ГАЛУЗЯХ ТА ВРАЗЛИВОСТЕЙ САЙТУ ALLTRANSUA

Хоча новітні підходи до розробки програмного забезпечення сприяють створенню складних програмних комплексів різного призначення, що характеризуються потужним спектром функціональних аспектів та належним рівнем надійності та захисту, проте за результатами дослідження міжнародної компанії Standish Group, функціональність та вимоги до якості ПЗ повністю забезпечена менш ніж в третині з усіх досліджених випадків, причому головною умовою було недопущення перевищення передбачуваного бюджету та термінів виконання проєкту. Хоча половина проєктів була реалізована успішно, проте це вартувало залучення додаткових ресурсів різного роду, зокрема була потреба у відтермінуванні проєкту та збільшення видатків, а 17-22% усіх проєктів взагалі були невдалими. Причинами цього були як недосконаліть та неефективність застосовуваних методів, так й інструментарію реалізації процесів інженерії програмного забезпечення. Тому актуальними задачами в цій галузі є залучення нових методів та засобів, що спрямовані на забезпечення якості кінцевого вдосконаленого продукту програмного забезпечення [2].

З кожним днем ландшафт загроз інформаційній безпеці набуває все більш складного та динамічного характеру, також зростає потреба у більшому моніторингу та сучасних заходах безпеки з ціллю випередження зловмисників. Наявні системи виявлення вторгнень в мережі стають все більш слабкими та уразливими проти нових видів загроз. Можливими рішеннями у вдосконаленні процесу виявлення аномалій та ідентифікації різних видів діяльності (в тому числі злочинної) є системи виявлення вторгнень на базі штучного інтелекту [3].

Сьогодні ландшафт загроз стає дедалі складнішим та динамічнішим, вимагаючи постійної пильності та інноваційних заходів безпеки, щоб випереджати кіберсупротивників. Системи виявлення вторгнень у мережі на основі сигнатур стають менш здатними виявляти нові загрози. Саме тому компанії з кібербезпеки в усьому світі інвестують величезні ресурси в розробку надійного підходу до виявлення мережевих загроз за допомогою алгоритмів

штучного інтелекту. Системи виявлення вторгнень на основі штучного інтелекту демонструють чудові результати у виявленні аномалій, ідентифікації діяльності або поведінки, що значно відхиляється від нормальних моделей. Потреба в системах на основі штучного інтелекту лише зростає.

Для проєктування системи безпеки для транспортного ресурсу AllTransUA було проаналізовано дослідження, що стосуються багатофакторної системи автентифікації, які дадуть змогу зменшити ризик зламу акаунтів, а також розглянуто джерела в галузі політики паролів. Дослідження в галузі перевірки на метадані дадуть змогу зрозуміти, як буде найбільш вигідно реалізувати механізми, що унеможливлять або принаймні ускладнять публікацію контенту, що не відповідає тематиці ресурсу. Результати аналізу джерел, що були присвячені процесу журналювання даних, будуть в подальшому застосовані при організації процесу журналювання процесу зміни привілеїв адміністрацією та задля зменшення зловживання адміністративним ресурсом. Окрім цього, в даному розділі було проведено аналіз наявних вразливостей сайту, що базувався на особистому багаторічному досвіді користування сайтом AllTransUA.

2.1 Аналіз досліджень в галузі багатофакторної автентифікації та політики паролів

Для дослідження власне явища багатофакторної автентифікації було досліджено статтю Дудикевича В., Микитин Г., Насилевського В. та Фігурняка В. [4]

Ключовими складовими систем автентифікації у веб-ресурсах є:

- суб’єкт (користувач);

- характеристика (пароль та біометричні реєстраційні дані, код з пристрою тощо);

- власник системи (замовник веб-ресурсу, а у випадку з AllTransUA, за сумісництвом ще й засновник);

- механізм автентифікації (програмне забезпечення (надалі – ПЗ) системи БФА), який у випадку AllTransUA відбувається всередині сайту або мобільного додатка AllTransUA;

- механізм керування доступом (обліковий запис та процес реєстрації).

Для забезпечення вимог конфіденційності, захисту та цілісності інформації можна використовувати різні фактори автентифікації або їх поєднання, зокрема: фактор знань (секретна інформація, відома лише власнику акаунта), фактор властивостей (біометричні дані), фактор власності (смартфон, стаціонарний, портативний комп'ютери та інші пристрої, генератор одноразових паролів).

В табл. 1 наведено способи автентифікації у веб-застосунках (включно і в додатку досліджуваного транспортного краудсорсингового медіа-порталу AllTransUA) [4].

Таблиця 1 – Порівняльна характеристика способів автентифікації у застосунках

Спосіб	Вимоги	Захищеність
Пароль	-	Середня
ЕЦП	Файл ЕЦП, спеціально підібраний пароль	Висока
СМС	Телефон, доступ до Інтернету	Висока
Біометрика	Додаток в телефоні, доступ до Інтернету, наявність додаткових засобів	Висока
Геолокація	Наявність спеціалізованих пристроїв	Середня
Технічні засоби	Наявність додаткових засобів	Висока
Пароль + СМС	Телефон, доступ до Інтернету	Висока
Пароль + біометрика	Наявність додаткових засобів, додаток в телефоні	Дуже висока
Пароль + ЕЦП	Файл ЕЦП, спеціально підібраний пароль	Висока
Біометрика + технічні засоби	Наявність додаткових засобів	Дуже висока
Пароль + технічні засоби	Наявність додаткових засобів	Висока

БФА поєднує певну кількість різних способів в довільному порядку, проте на практиці можна використовувати комбінації способів, серед яких найбільш ефективними вважаються поєднання паролю разом з ЕЦП, СМС або біометричними даними, завдяки чому забезпечується конфіденційність користувача [4].

Оскільки мова йде про сайт пізнавального характеру AllTransUA, то важливо поєднати і простоту механізму багатофакторної автентифікації, що приваблюватиме користувачів, і вищий рівень безпеки їхніх даних, тому вкрай важливо провести відбір найбільш ефективних способів реалізації БФА.

Очевидно, що автентифікація винятково через пароль є вкрай неефективною і легко піддається зламу. Автентифікація через ЕЦП хоча і є більш надійним та більш стійким до атак способом автентифікації, проте такий механізм не є простим у застосуванні, адже далеко не всі користувачі мають електронно-цифровий підпис, що є абсолютно недоречним у випадку пізнавальної ролі сайту краудсорсингової платформи AllTransUA. Не рекомендується також з точки зору безпеки використовувати автентифікацію через SMS попри доволі простий механізм автентифікації: по-перше, послуги мобільних операторів є платними, що означає, що під час кожного сеансу входу буде стягуватися плата, по-друге, такий тип автентифікації вразливий проти атак SIM-swap. Окрім цього, неефективною є також автентифікація через геолокацію, передусім, через неточність (з одної місцевості можуть заходити декілька користувачів, особливо у випадку з пристроями загального користування), а також, можливість змінювати геолокацію через використання віртуальних приватних мереж (VPN). Автентифікація через технічні засоби (апаратні ключі) також ускладнює процес користування сайтом (є доступними далеко не кожному користувачеві), хоча і гарантує захист від фішингу та вищий рівень безпеки користувачів. Комбінація ЕЦП/СМС та паролю є неефективною з тих самих причин, що і у випадку з автентифікацією через ЕЦП та СМС. Також недоцільними є методи автентифікації через технічні засоби в поєднанні з паролем та біометрикою, адже як вже згадувалося, апаратні ключі доступні далеко не кожному користувачеві,

що суперечить потребам сайту краудсорсингової транспортної платформи AllTransUA.

Таким чином найкращими методами автентифікації залишаються біометрика та комбінація біометричних даних та паролю.

Окрім цього, також потенційно можливим рішенням може вважатися технологія TOTP (Time-based One Time Password), тобто одноразовий тимчасовий пароль, що діє лише впродовж короткого періоду часу як свого роду другий фактор автентифікації для забезпечення БФА.

Найкращим зразком втілення такої технології є додаток Google Authenticator, вказаний на рис. 2.1 [5], а для біометричної автентифікації існує додаток Дія.Підпис, вказаний на рис. 2.2 [6]:

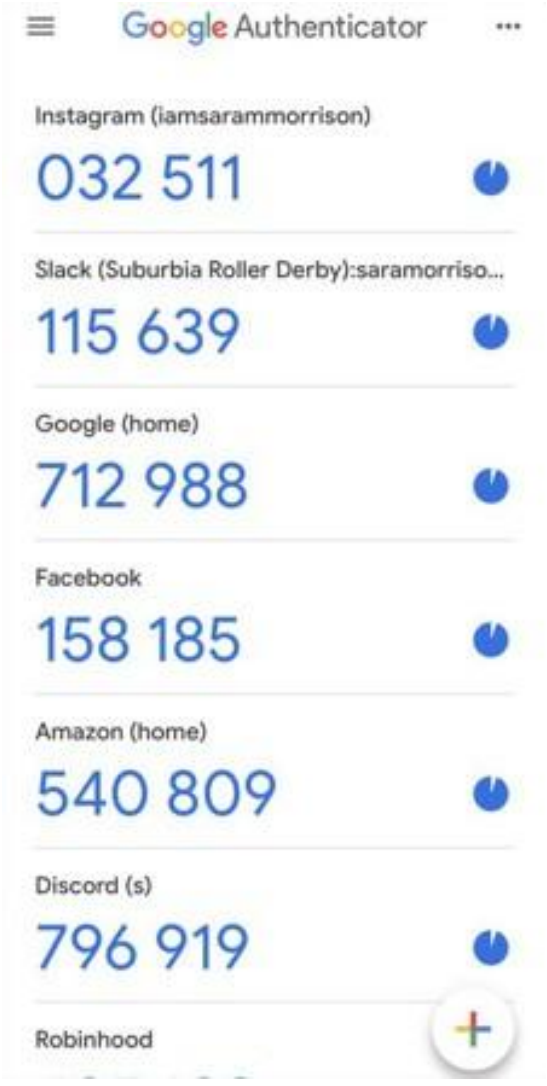


Рисунок 2.1 – Знімок додатка Google Authenticator для багатофакторної автентифікації [5]

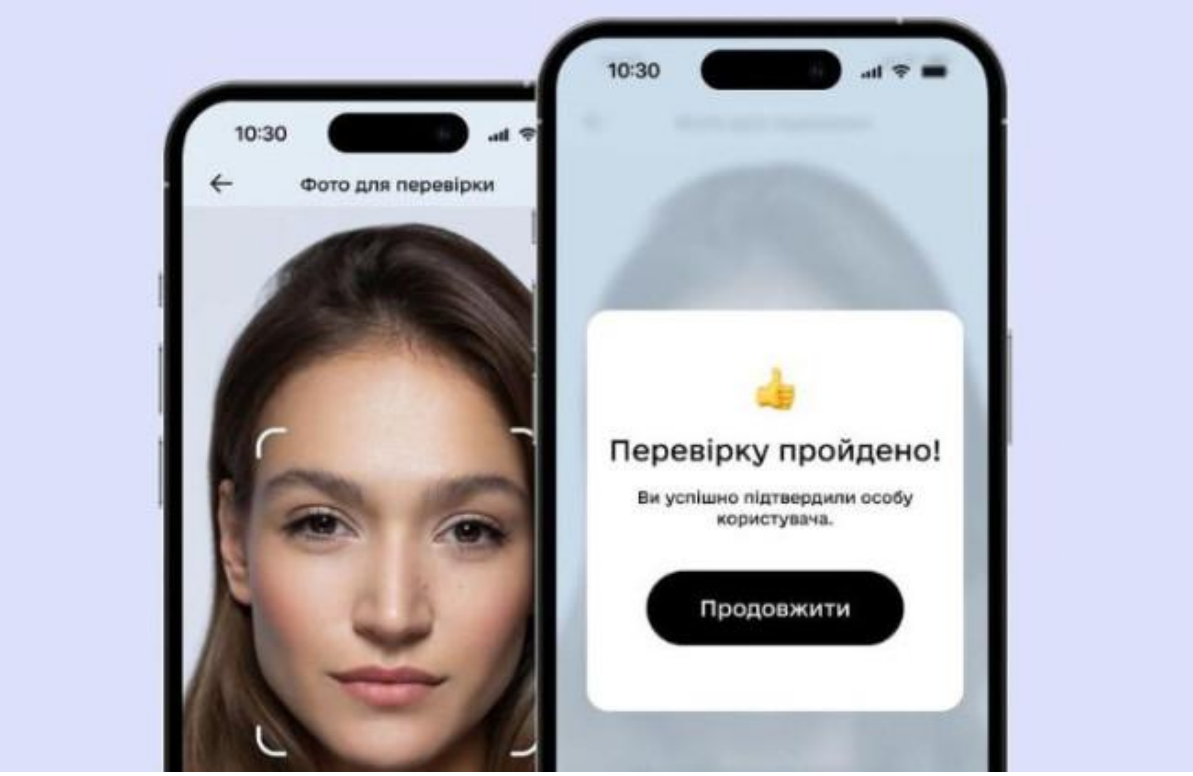


Рисунок 2.2 – Біометрична автентифікація через додаток Дія.Підпис [6]

Також важливим є питання політики паролів, оскільки більшість користувачів не переймається питаннями, наскільки їхній пароль є потужним та стійким до зламу. Так, в дослідженнях Гадяцької Ю. зазначається, що паролі залишаються не лише найпоширенішим, а й одним з найбільш слабких місць інформаційної безпеки, адже зловмисники сьогодення зламують та отримують НСД до паролів різними методами [7]. Серед них варто виділити:

- метод брутальної сили (brute-force attack) або силового перебору символьних комбінацій для паролів;

- фішингові листи через підроблену електронну пошту та веб-сайти;

- соціальна інженерія (отримання паролів через психологічні прийоми).

Політикою паролів називають документ, що визначає та формує правила створення, зміни та контролю паролів в інформаційних системах. Наявність його є вкрай важливою вимогою захисту інформації, оскільки дає змогу забезпечити надійність та ефективність системи захисту.

Політика паролів є одним з можливих засобів інформаційного захисту проти таких загроз, передусім завдяки наступним інструментам, зокрема:

- надійність паролів (вимоги та правила створення паролів)

- унікальність паролів (правила зміни паролів)

- контроль паролів (відхилення слабких паролів)

Для цього важливо розробити правила паролів, які забезпечуватимуть та гарантуватимуть їхню надійність та унікальність. Серед основних вимог існують нижче наведені правила: по-перше, довжина пароля повинна становити не менше ніж 12 символів, по-друге, повинен бути не один набір символів, а декілька, наприклад, комбінація з літер, цифр, символів пунктуації та інших категорій символів, і по-третє, пароль не повинен бути простим словом, фразою, числом (вкрай не бажано впроваджувати паролі типу “1234”, “1111”, “abcd” та інші легкі для запам’ятовування набори символів) та не повинен бути пов’язаний з особистою інформацією користувача (дата народження, місце проживання, ім’я, по-батькові, прізвище та інші).

Важливо подбати про надійне зберігання паролів, щоб захистити їх від помічення сторонніми особами. Для цього можна використовувати такі методи:

- запам’ятовування в голові

- зберігання паролів в зашифрованому вигляді на зашифрованих носіях інформації

- зберігання паролів в ПЗ для забезпечення для управління паролями

Щоб паролі було важче зламати, їх потрібно регулярно змінювати, не рідше ніж один раз на 90 днів. Система повинна перевіряти паролі на надійність шляхом перевірки на їхню наявність в базі відомих паролів, на наявність в паролях простих слів та/або фраз та на наявність зв’язку з особистими даними користувача [7].

2.2 Аналіз досліджень в галузі перевірки на мета-дані (розпізнання об’єктів на фото)

Для розуміння, як втілювати перевірку фото на мета-дані та перевірку наскільки фотоматеріали відповідають тематиці ресурсу AllTransUA, було проаналізовано та досліджено джерела в галузі розпізнавання об’єктів.

Так, згідно статті авторства Бондаренко К. О., Гнідунця В. О. та Крупельницького В. О. [8], справедливо зауважено, що інформаційні технології в галузі розпізнання об’єктів на фотографіях набувають все ширшого застосування, адже такі системи здатні обробляти та аналізувати візуальні дані, які можна застосувати в перспективі в різних галузях життєдіяльності. Яскравими зразками таких систем можуть слугувати згаданий в пп. 2.1 додаток Дія.Підпис, що здійснює верифікацію особи через біометричні дані (сканування обличчя), а також всім відомі системи відеоспостереження для забезпечення безпеки, автономні транспортні системи (зокрема і засоби фіксації порушень ПДР, що ідентифікують транспортний засіб та номерний знак, як на рисунку 2.3) [9].

Рисунок 2.3 – Перевірка об’єктів на фото на прикладі простої фіксації порушень ПДР [9]

За подібним принципом працює і механізм бот-перевірки reCAPTCHA, який при проходженні власне бот-перевірки вимагає або ввести символи з зображення, як на рис. 2.4 [10], або вибрати зображення, на яких зображені транспортні засоби (в тому числі автобуси), знаки ПДР, гідранти або інші об’єкти, як на рис. 2.5 [11]:

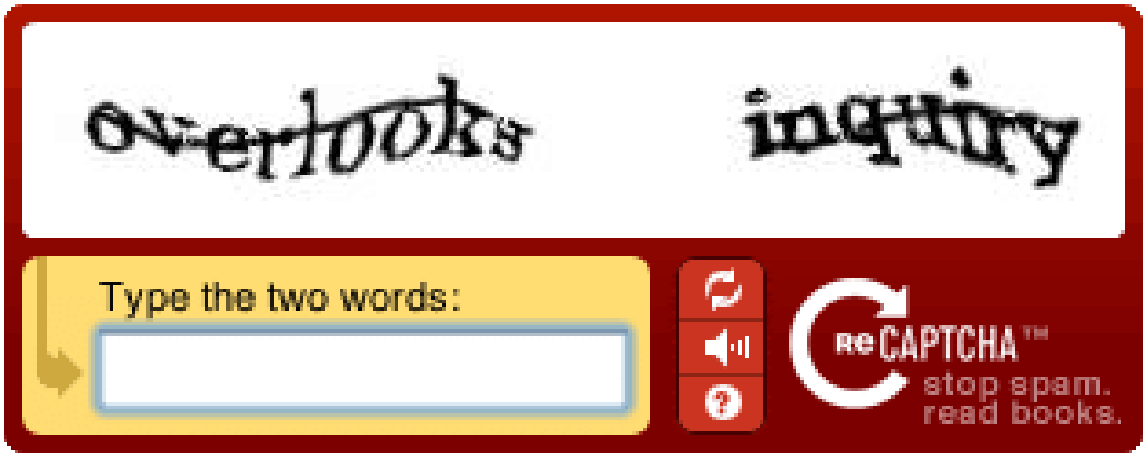


Рисунок 2.4 – Перевірка даних на фото на прикладі механізму reCAPTCHA: введення тексту та перевірка збігів з контентом на фото [10]

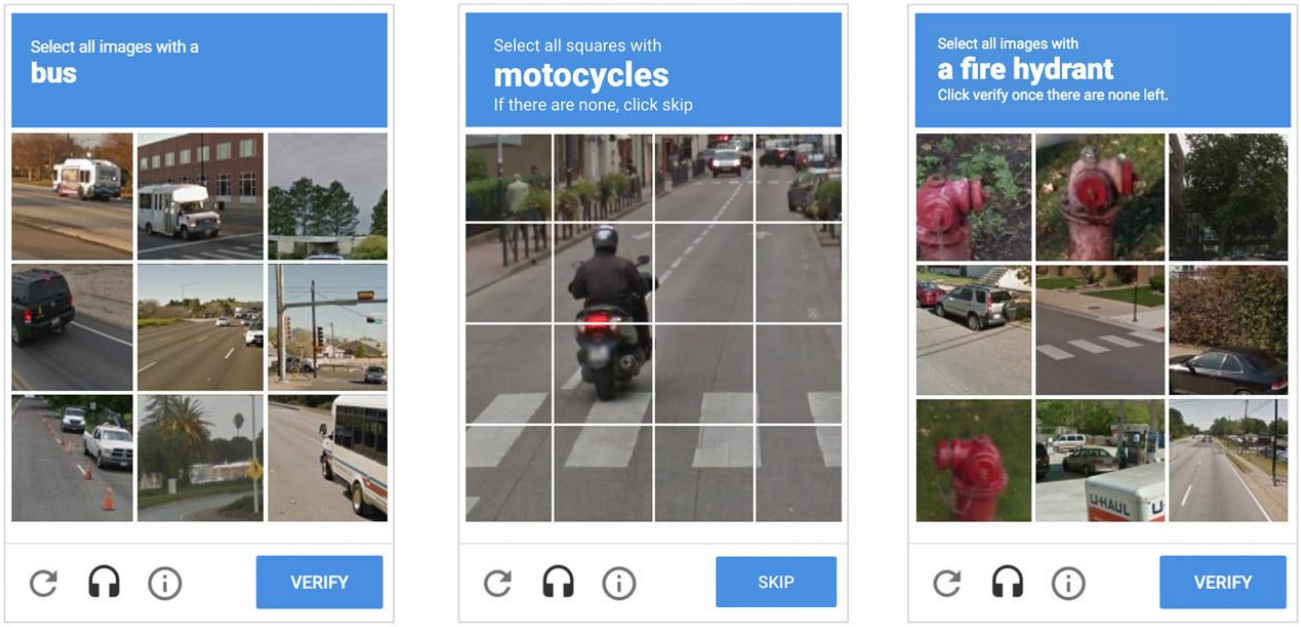


Рисунок 2.5 – Перевірка об’єктів на фото на прикладі механізму reCAPTCHA: вибір зображень з певними типами об’єктів [11]

Таким чином, бот-механізм також оперує об’єктами та даними, зображеними на фотографіях, тож цілком імовірно такі механізми і є можливим рішенням для впровадження перевірки фотографій на наявність транспортних засобів на фото.

2.3 Аналіз досліджень в галузі журналювання даних

Для розуміння важливості процесу журналювання було проаналізовано статтю Stanciu N., присвячену аналізу важливості керування журналом подій для забезпечення безпеки інформаційної системи [12].

У цій статті огляд журналів подій представлений як компонент аудиту інформаційної системи, також описано важливість таких журналів та способи їх аналізу для оцінки ефективності контролю функціоналу інформаційної системи, а також описано загальний інструмент управління інформацією та подіями безпеки, відомий також як SIEM (Security Information And Event Management), що відповідає за збір журналів подій, що генеруються різними джерелами, наприклад, журнали безпеки ПЗ, журнали ОС та журнали власне ПЗ [12].

Як вже зазначено авторами цієї публікації, швидкий процес розширення можливостей інформаційних технологій сприяв як і здобуткам для бізнесу та організацій, так і загрозам безпеці, в тому числі і вторгнення та проникнення в систему, розподілена відмова в обслуговуванні, що має все більш руйнівний вплив на функціонування інформаційних систем. Тому процес вдосконалення журналювання подій безпеки є вкрай необхідним для зменшення обсягу втрат та збитків та впровадження заходів із зниження рівня ризику.

Із зростанням кількості та обсягів мережевих серверів та інших обчислювальних пристроїв відбулося також помітне зростання обсягів, кількості та різноманітність журналів комп’ютерної безпеки. Журнали подій є важливою складовою процесу аудиту та виявлення вторгнень, а також є набором записів активності в інформаційній системі (зокрема, процесів в програмному забезпеченні та активності користувачів) і використовуються процесами аудиту для аналізу та оцінки ефективності процесів контролю [12].

Також, згідно досліджень в статті авторства Mohamed A. El-Zawawy, що датуються 2025 роком, було досліджено ризик прихованого незаконного підвищення привілеїв з боку програм (подібні ризики мають місце і в краудсорсинговій транспортній платформі AllTransUA, хоча зловживання відбувається не з боку ПЗ, а адміністрації сайту) [13].

Так, попри те, що система дозволів Android обмежує доступ і захищає користувацькі дані, недоліки системи безпеки дозволяють зловмисному ПЗ зловживати дозволами. Одним із найбільш основних недоліків системи безпеки і є незаконне підвищення привілеїв [13].

Підхід, запропонований Mohamed A. El-Zawawy, ідентифікує на систематичній основі багатоетапні незаконні підвищення привілеїв за допомогою автоматизованого формування тест-кейсів та стаціонарного аналізу [13].

В ході досліджень було також встановлено важливу відмінність: доброякісне ПЗ більші привілеї отримують поступово через ланцюжки ескалації, в той час як зловмисне ПЗ з самого початку запитують надмірно високі привілеї без поступового підвищення привілеїв. Така відмінність вкотре підтверджує необхідність у вдосконаленні методів управління дозволами для зменшення ризиків, пов’язаних з незаконним підвищенням привілеїв, які зазвичай ігноруються сучасними системами IDS (Intrusion Detection System) / IPS (Intrusion Prevention System) [13].

Досліджені джерела ілюструють важливість не лише самого процесу журналювання, а і його вдосконалення з ціллю зниження рівнів ризиків, пов’язаних з незаконним прихованим підвищенням привілеїв.

2.4 Аналіз вразливостей кожного з безпекових аспектів системи

2.4.1 Публікація матеріалів та система модерації

Завдяки наявності на сайті AllTransUA описаної в підрозділі 1.4 премодерації за замовчуванням з моменту створення облікового запису існує можливість безперешкодно завантажувати контент. Ця обставина тягне за собою дві крайнощі: з одного боку, це не демотивує публікувати та ділитися власними фотоматеріалами користувачів, що уже мають досвід публікації на інших ресурсах і формує позитивний імідж досліджуваного транспортного ресурсу поміж краудсорсингових платформ, створених в інших країнах світу (наприклад,

seznam-autobusu, що походить з Чехії, польський транспортний медіа-ресурс phototrans.eu та інших), з іншого боку, це відкриває шлях для зловживань з боку окремих користувачів, які починають систематично і масово публікувати неетичний контент, що в свою чергу, додає зайвого навантаження фотомодераторам, відповідальним за фільтрацію та прийняття рішень щодо фотографій. Здебільшого неетичний контент проявляється в публікації образливих, нецензурних фотоматеріалів, які не відповідають транспортній тематиці ресурсу, як вказано на рис. 2.6 та рис. 2.7:

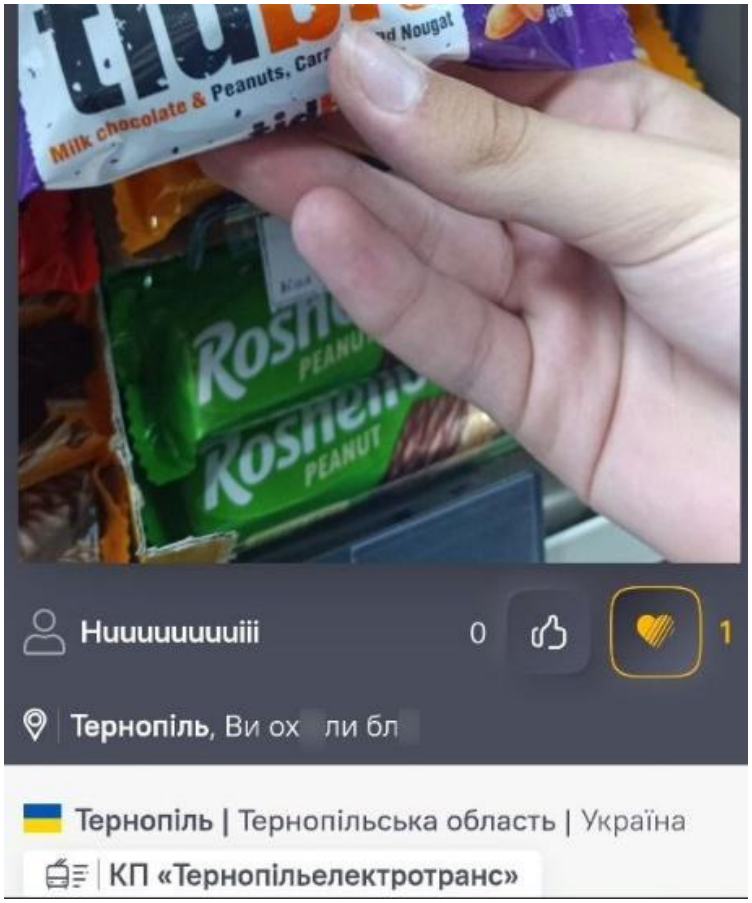


Рисунок 2.6 – Ризик, зумовлений відсутністю перевірки на метадані: користувач №1 публікує нецензурну лексику при вказанні місця зйомки

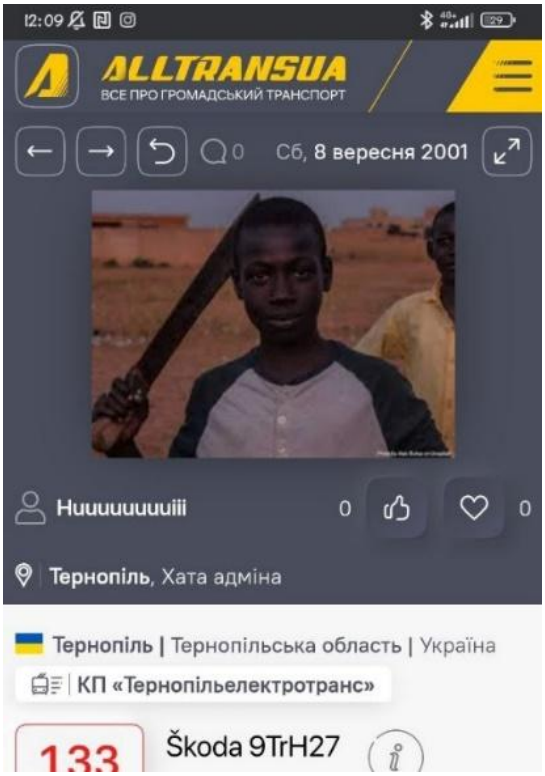


Рисунок 2.7 – Ризик, зумовлений відсутністю перевірки на метадані: користувач №1 публікує контент, що не відповідає тематиці транспортного додатку AllTransUA

Така проблема зумовлена передусім відсутністю автоматизованої перевірки фотоконтенту на метадані (наявність транспортних засобів). Впровадження автоматизованої перевірки зображень надасть змогу зменшити обсяг роботи фотомодераторам і зосередитися на основній частині їхньої діяльності, а саме фільтрації та прийнятті рішень стосовно фотографій, що відповідають тематиці ресурсу (схвалювати фотографії достатньо прийнятної якості/цінності, відправляти на доопрацювання фотографії недостатньої якості, які підлягають відновленню та відхиляти фотографії критично низької якості). Ручна перевірка (себто людська праця) хоча і є також можливим рішенням, проте має свої нюанси у вигляді людського фактора (існує імовірність, що невідповідний тематиці контент можуть прийняти з необачності, в розважальних цілях тощо) та ризиків упередженої поведінки модераторів стосовно особи / групи осіб. Таким чином, найкращим рішенням є впровадження автоматизованої перевірки на метадані, що забезпечить відчуття суспільства, що для всіх правила є однаковими,

незалежно від статі, віку, місця проживання, посади та інших користувацьких чинників.

2.4.2 Журналювання

На сайті AllTransUA наразі діє лише журналювання змін даних, згадане в підрозділі 1.5, при цьому відсутнє журналювання змін привілеїв, що породжує ризики зловживання адміністративним ресурсом у вигляді прихованого незаконного підвищення та позбавлення привілеїв користувачів з різних причин без відома інших користувачів, що може мати місце серед адміністрації сайту, зокрема на основі особистого ставлення адміністраторів до конкретної особи / групи осіб.

Згаданий ризик формує відчуття відсутності справедливого адміністрування сайту у користувачів нижніх ланок (модераторів, редакторів та пересічних користувачів), сприяє погіршенню атмосфери в спільноті користувачів сайту AllTransUA, включно й на іноземних користувачів та загального іміджу та соціального рейтингу сайту.

2.4.3 Механізми реєстрації, автентифікації та авторизації

На сайті діє наразі лише двофакторна автентифікація, що передбачає вхід та реєстрацію лише за електронною поштою, логіном та паролем. Окрім цього, на сайті відсутня політика паролів при створенні облікових записів Як показує така практика, такі дані доволі легко зламати, особливо якщо пароль є доволі слабким і надто простим у запам’ятовуванні.

Відсутність багатофакторної автентифікації породжує ризик злому сторінки, а це, в свою чергу породжує наступні ризики, особливо, якщо зламано обліковий запис користувача, що не перебуває на премодерації контенту (хакер таким чином підставляє жертву перед адміністраторами в аспекті відповідальності за скоєне порушення та підрив довіри адміністрації до користувача), включно і вже згадані ризики, зумовлені недоопрацьованою системою постмодерації: витік конфіденційної / особистої інформації,

поширення інформації, що не підлягає поширенню (інформація з грифами секретності різних категорій), поширення недостовірної інформації, використання системи пост-модерації з ціллю дискредитації певної особи / групи осіб, що може спричинити побоювання та панічні настрої серед усіх користувачів платформи AllTransUA, а також створення ще декількох посторонніх облікових записів, що дозволяє здійснювати подальші атаки на сайт, що видно на рис. 2.8.

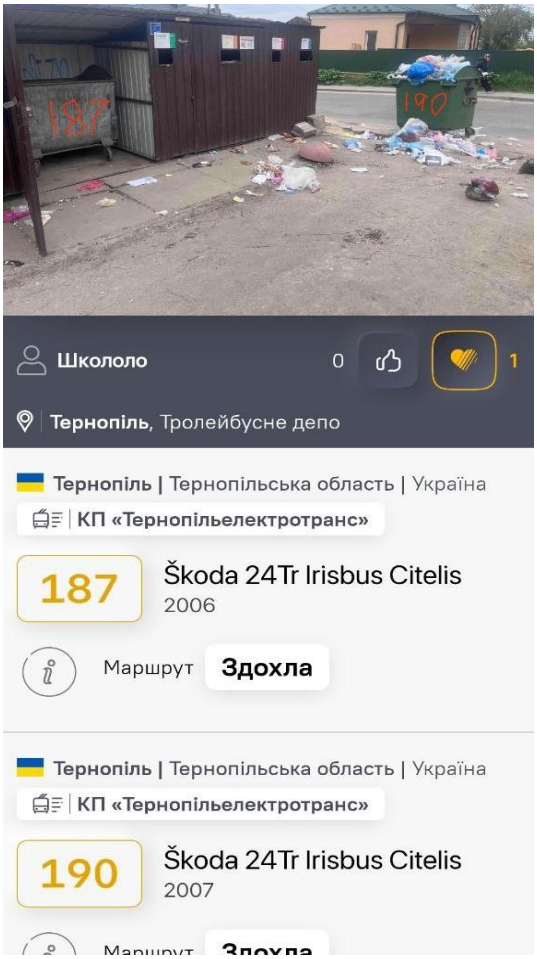


Рисунок 2.8 – Ризик, зумовлений відсутністю багатофакторної автентифікації на медіа-порталі: користувач №2 публікує контент, що не відповідає тематиці транспортного додатку AllTransUA

Враховуючи вищезгадані прецеденти та дослідження, проведені в розділі 1 підпунктах підрозділу 2.4 та дослідження, проведені в попередніх трьох підрозділах, в наступному (третьому) розділі було розроблено проєкт системи

безпеки для кожного дослідженого функціонального аспекту сайту AllTransUA та загальний проєкт системи безпеки сайту.

2.5 Висновки до другого розділу

В ході аналізу джерел, присвячених багатофакторній автентифікації та політиці паролів, було проаналізовано всі способи реалізації БФА за їх фактичною ефективністю та простотою імплементації та подальшої експлуатації на сайті краудсорсингової транспортної платформи AllTransUA.

Встановлено, що найбільш ефективним способом реалізації БФА є автентифікація через пароль та TOTP (Time-based One-Time Password) одноразовий код, який діє впродовж доволі короткого періоду часу, а інші методики є або платними та уразливими проти атак на SIM-карту (всі способи із застосуванням SMS-повідомлень), або значною мірою ускладнюють користування сайтом (всі способи із застосуванням технічних засобів та/або ЕЦП), або взагалі є неточними (застосування геолокації), а також із застосуванням біометричних даних (за схожим принципом до додатка Дія.Підпис, проте без вікових обмежень, адже в додатку можуть реєструватися лише особи, яким виповнилося 14 років).

Також було встановлено, що для захисту облікових записів від отримання НСД зловмисниками важливо також впроваджувати політику паролів, яка відхилятиме надто прості паролі та передбачатиме потребу їхньої зміни впродовж певного проміжку часу, щоб зменшити ризики зламу паролів.

Дослідження джерел, присвячених перевірці зображень на дані, а саме розпізнанні об’єктів на фото, демонструють, що такі системи мають широке застосування, і їх можна застосовувати в багатьох галузях життєдіяльності, включно і на сайті краудсорсингової транспортної платформи AllTransUA. Подібний принцип розпізнання об’єктів на фото втілюється в засобах фіксації порушень ПДР та ТЗ-порушників, а також в системі бот-перевірки reCAPTCHA (при введенні тексту із фотографії та виборі фотографій з певними об’єктами на фото).

На прикладі досліджень в галузі журналювання було продемонстровано, що із зростанням рівня розвитку інформаційних систем зростає потреба в більш якісному управлінні даними та збільшенні обсягів журналювання даних. Дослідження в галузі прихованого зловживання привілеями також показали, що потрібно вести і журналювання змін привілеїв задля запобігання незаконному підвищенню привілеїв.

Проведені дослідження в майбутньому можна буде на практиці застосувати для усунення вразливостей, описаних в підрозділі 2.4, серед яких є і ризик обходу бану та публікація невідповідного тематиці сайту контенту.

РОЗДІЛ 3 ФОРМУВАННЯ ПРОЄКТУ СИСТЕМИ БЕЗПЕКИ САЙТУ ALLTRANSUA

3.1 Побудова системи безпеки сайту AllTransUA

Зі зростанням складності програмних систем стає все складнішим процес задоволення вимог якості в процесі проєктування ПЗ. Можливим рішенням з мінімумом втрат є перенесення цього процесу на стадію проектування архітектури, яка розглядається як сукупність компонентів та зв'язків, що забезпечують взаємодію між компонентами Оскільки чинна архітектура ПЗ (описана в ході досліджень, проведених впродовж усього першого розділу) є вискорівневою моделлю для представлення будови програмної версії сайту (сайт AllTransUA має також свій програмний додаток) та її основних компонентів, її вибір є підставою для вдосконалення якості програмного забезпечення досліджуваного сайту [14].

Даний розділ присвячений безпосередній розробці проєкту системи захисту користувацьких даних на сайті краудсорсингової транспортної платформи AllTransUA для найбільш важливих і вразливих аспектів функціонування ресурсу. Важливо зазначити, що дослідження будуть присвячені саме розробці проєкту системи безпеки, оскільки вони виконувалися в умовах відсутності доступу до адміністративного ресурсу.

3.1.1 Багатофакторна автентифікація та політика паролів

Для вдосконалення механізмів автентифікації було розроблено проєкт системи безпеки, в якому було застосовано дослідження, проведені в підрозділі 2.1. В ході аналізу вищезгаданих досліджень було розроблено креслення проєкту імплементації багатофакторної автентифікації та політики паролів, зображеного на рисунку 3.1 на наступній сторінці:

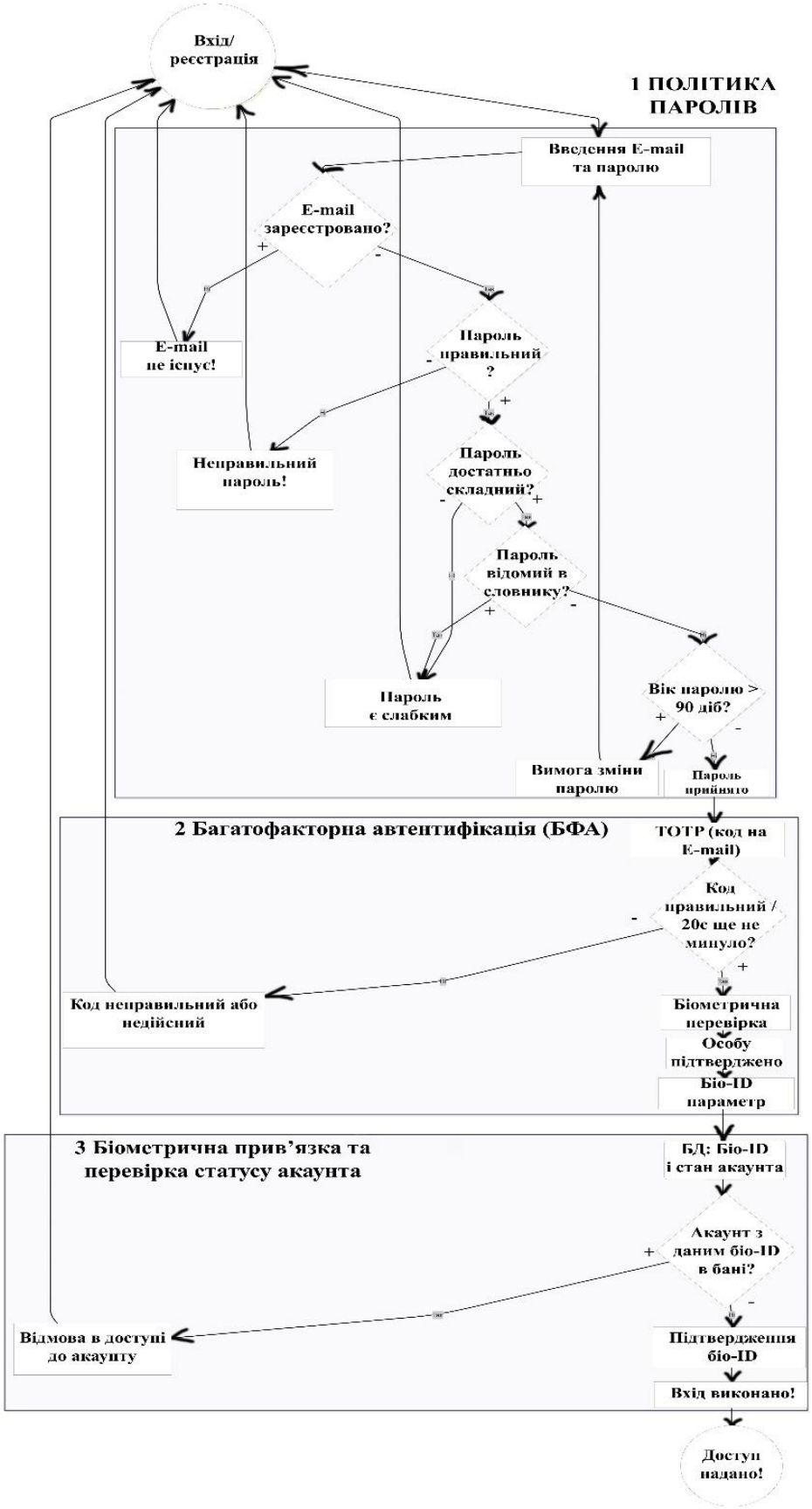


Рисунок 3.1 – Проєкт БФА

Дослідження, проведені в підрозділі 2.1, довели, що найкращою і водночас найпростішою формою автентифікації вважається система, що комбінує в собі і

уже наявну систему автентифікації через логін та пароль, і автентифікацію через короткочасний одноразовий код (TOTP або Time-based One Time Password), що приходить на електронну пошту користувачеві, і автентифікацію через біометричні дані. З ціллю безпеки і зменшення імовірності перехоплення пароля було прийнято рішення встановити термін дії одноразового пароля в 20 секунд – цього часу цілком достатньо, щоб зайти в електронну пошту, скопіювати/запам’ятати код і ввести його під час автентифікації.

Після автентифікації через TOTP-пароль проєктом передбачена процедура біометричної автентифікації (через фіксацію обличчя або відбиток пальця як більш унікального біометричного параметра), в ході якої користувач фактично підтверджує свою особу. Пропонується обліковувати біометричні параметри для ведення реєстру дозволених та заблокованих користувачів – якщо користувач має два акаунти, то у разі блокування одного з них в реєстрі біометричний параметр також блокується, а разом з ним блокується і другий акаунт. Як показує практика, деякі користувачі сайту AllTransUA мають по два акаунти, один з яких призначений для публікації фотографій суто для наповнення бази даних, інший призначений для публікації художніх фотографій, що загалом не є забороненим, але відкриває шляхи до зловживань.

Прив’язка облікових записів до єдиного біометричного параметра запобігає спробам створення обхідних облікових записів для подальшого здійснення зловживань та порушень правил сайту, значно ускладнюючи отримання НСД до акаунту зловмисником.

3.1.2 Аналіз контенту на мета-дані

За результатами досліджень, проведених в розділі 2.2, присвячених перевірці фото на мета-дані, було побудовано проєкт-схему пропонованої схеми модерації фотографій.

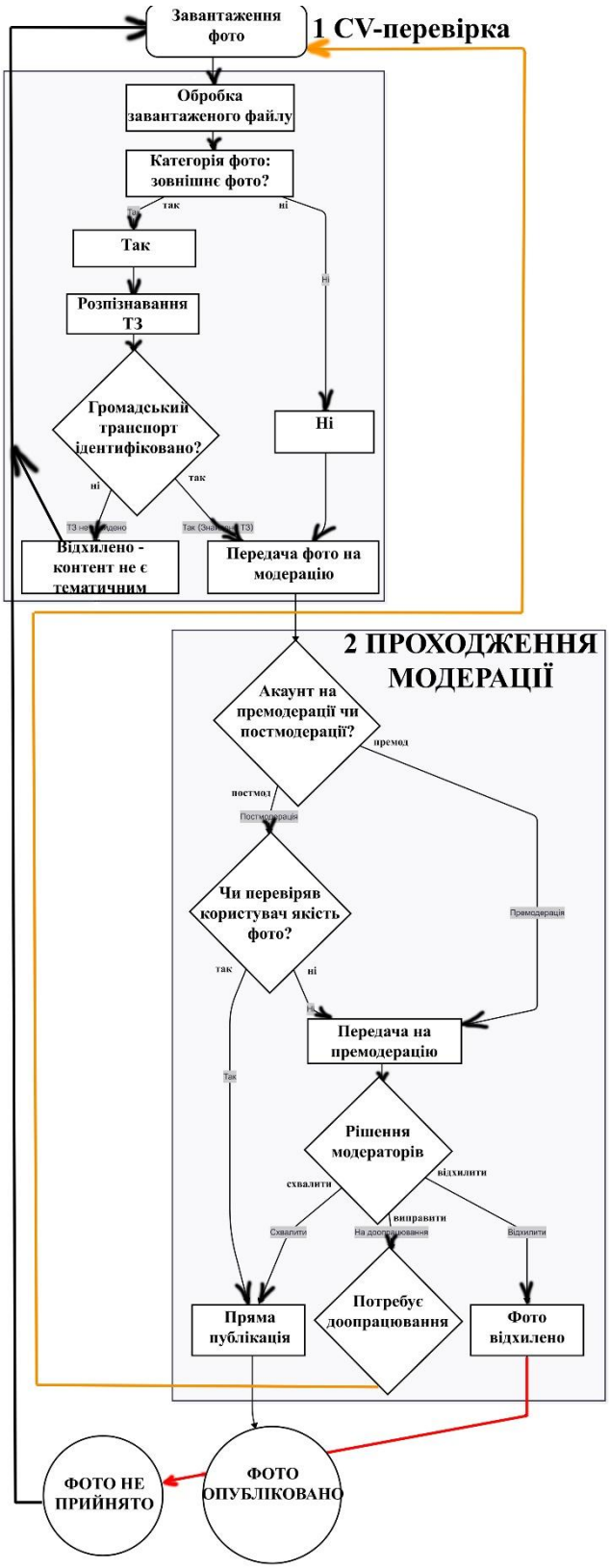


Рисунок 3.2 – Проєкт системи перевірки на мета-дані (розпізнання об’єктів на фото)

Як вже згадувалося в підрозділі, присвяченому аналізу вразливостей краудсорсингової платформи AllTransUA, на сайті мали і мають місце ризики зловживання системою модерації, яка передбачає публікацію фото на умовах

постмодерації за замовчуванням, а саме публікація контенту, що не відповідає тематиці сайту. Як часткове рішення цієї проблеми було запроваджено здійснення перевірки фотографій категорії “Зовнішнє фото”, адже більшість фотографій, що публікується на сайті, належать саме до цієї категорії.

Згідно проєкту системи перевірки на мета-дані, фотографія має спершу пройти автоматизоване розпізнання об’єктів на фотографії (всіх видів громадського транспорту: автобусів, тролейбусів, трамваїв, метрополітену, фунікулеру та інших видів ТЗ). Якщо фотографія цю перевірку не проходить, вона автоматично відхиляється.

Вже після проходження перевірки на мета-дані фото передається на модерацію, механізм якої було описано в підрозділі 1.4 і результати якої залежать безпосередньо від якості опублікованої фотографії.

3.1.3 Журналювання подій: прозора зміна привілеїв

Система журналювання даних наразі, як вже згадувалося в підрозділі 2.4, веде фіксацію лише змін в базі даних рухомого складу, при цьому відсутня процедура журналювання змін привілеїв, що породжує ризики, пов’язані з зловживанням адміністративним ресурсом, зокрема, незаконне підвищення та зниження привілеїв. На рисунку 3.3 представлено запропонований проєкт-схему журналювання, який можна буде на практиці застосувати як рекомендацію адміністрації сайту AllTransUA:

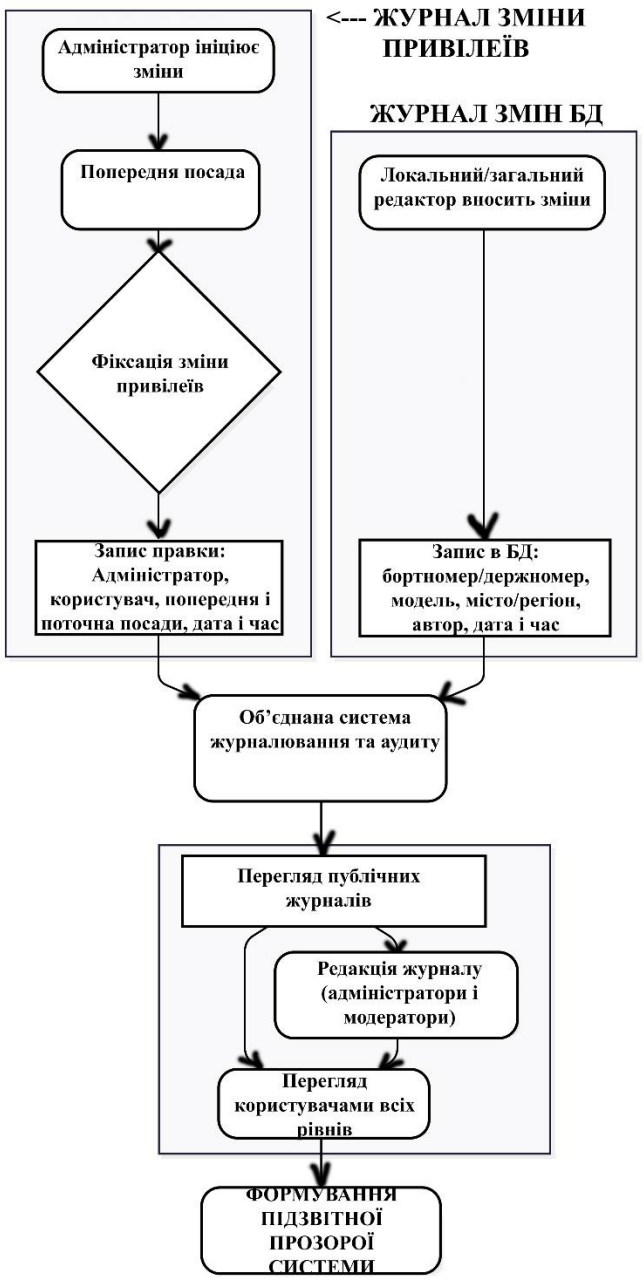


Рисунок 3.3 – Проєкт системи журналювання даних

Загалом пропонується в журналі фіксувати такі дані: адміністратор, який вніс зміни в привілеї, користувач, стосовно якого було вжито змін, попередній набір привілеїв і поточний набір привілеїв, дата та час внесення правок, а користувачі можуть переглядати і в разі потреби оскаржувати несправедливе підвищення/зниження своїх або повноважень інших користувачів. Оскільки на сайті AllTransUA користувачі можуть мати дві та більше посад одночасно, як вказано на рис. 3.1 на прикладі користувача, що має посаду адміністратора, локального редактора та модератора коментарів, пропонується фіксувати кожну зміну привілеїв в журналі:

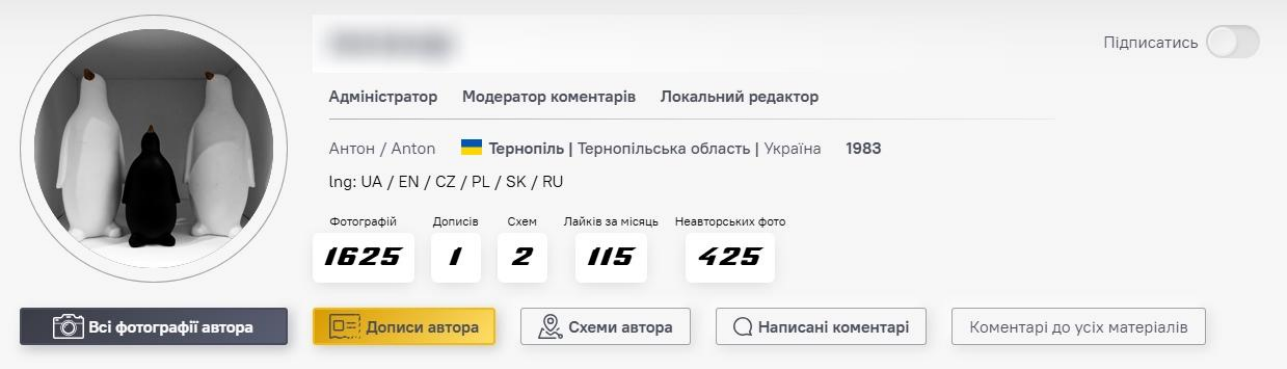


Рисунок 3.4 – Користувач, що може володіти декількома привілеями одночасно

В рамках проекту цієї схеми пропонується також впровадження уніфікованої об’єднаної системи журналювання та аудиту, де користувачі можуть відстежувати як і зміни в базі даних флоту РС, так і зміни адміністраторами повноважень інших користувачів, що є одним з можливих способів забезпечення прозорості та зменшення ризиків зловживання адміністративним ресурсом з боку адміністрації.

3.1.4 Побудова загального проєкту системи безпеки

Також в ході досліджень було розроблено загальний проєкт системи безпеки, який є коротким представленням усіх розроблених проєктів, створених в ході досліджень: проєкту системи БФА та політики паролів, проєкту перевірки фото на мета-дані (розпізнання об’єктів на фотографіях) та системи журналювання даних. Він поєднує в собі усі розроблені проєкти, детальний план та пояснювальна записка до яких наведені в попередніх пунктах підрозділу і представлений в рисунок 3.5

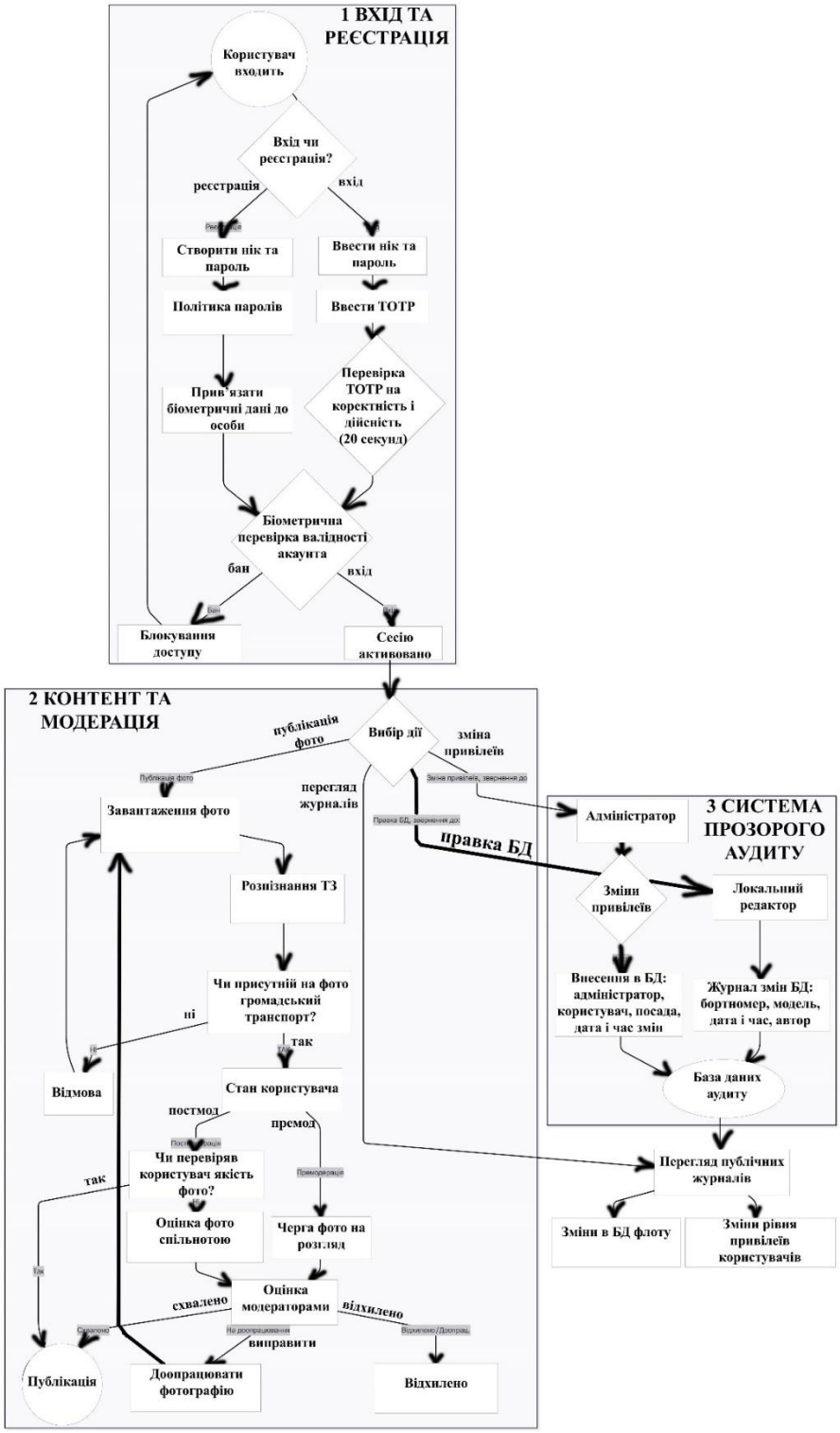


Рисунок 3.5 – Загальний проєкт системи безпеки сайту AllTransUA

Згідно загального проєкту системи безпеки для сайту AllTransUA, перш ніж отримати доступ та користуватися послугами та функціями сайту, користувач повинен зареєструватися і створити достатньо стійкий проти зламу пароль, інакше в доступі йому буде відмовлено. Потім йому потрібно буде прив’язати акаунт до біометричних даних (фіксацію обличчя або відбитка пальців як більш

унікального біометричного параметра) для остаточного підтвердження особи, після чого його унікальний біометричний ідентифікатор заноситься в БД біометричних ідентифікаторів. Якщо згаданий ідентифікатор знаходиться в чорному списку, особі буде відмовлено в доступі.

Якщо входить в сайт зареєстрований користувач, йому буде необхідно пройти автентифікацію через одноразовий пароль TOTP, а потім знову пройти біометричну верифікацію своєї особи – функціонал там схожий до випадку з реєстрацією на сайті. Детальніший опис проекту функціонування системи автентифікації можна глянути в пункті підрозділу 3.1.1 з відповідним кресленням.

Якщо особа не перебуває в чорному списку сайту AllTransUA, вона отримує доступ до функцій сайту AllTransUA, зокрема, до публікації фотографій, дописів та коментарів.

Оскільки наразі на сайті існують ризики публікації нетематичного контенту, то з ціллю полегшення роботи фотомодераторам і зменшення обсягів засмічування галереї пропонується ввести автоматизовану перевірку фотографій на мета-дані (розпізнання об’єктів на фото) – якщо фотографія її проходить, вона після цього проходить процес модерації, описаний детальніше в пункті підрозділу 3.1.2, згідно якого є три кінцеві варіанти розвитку подій: прийняття фотографії, відправлення на доопрацювання або відхилення фотографії.

Додатковим компонентом функціонування сайту, який доступний кожному користувачеві і який також пропонується вдосконалити – система журналювання даних, яка детальніше описана в пункті підрозділу 3.1.2. Для цього пропонується впровадити систему журналювання змін привілеїв (повноважень) користувачів, передусім з ціллю запобігання зловживання адміністративним ресурсом та прозорого обліку змін привілеїв, щоб користувачі могли переглядати і в разі потреби оскаржити неправомірне підвищення або зниження повноважень відносно свого акаунту або інших користувачів, а кожну зміну привілеїв фіксувати у відповідному журналі, оскільки користувачі можуть обіймати дві та більше посад на досліджуваному сайті AllTransUA, зокрема, обліковий запис

адміністратора, який вносив зміни, обліковий запис користувача, щодо якого проваджувалися зміни, попередні та поточні посади, а також час та дату правок.

3.2 Висновки до третього розділу

На основі досліджень джерел, присвячених відповідним тематикам та аналізу вразливостей джерел було розроблено проєкти найбільш уразливих функціональних компонентів сайту краудсорсингової платформи AllTransUA, а саме механізмів реєстрації та входу, системи модерації та журналювання даних.

В ході дослідження було встановлено, що користувачі можуть мати по два і більше облікових записів – хоча це не заборонено, але в умовах чинних механізмів реєстрації та входу це слугує плацдармом для зловживань та здійснень атак на сайт AllTransUA, а також отримання хакерами несанкціонованого доступу до облікових записів користувачів. Для вдосконалення механізмів реєстрації та входу було розроблено проєкт, згідно якого пропонується додатково до уже наявних реєстраційних даних впровадити систему багатофакторної автентифікації за одноразовим паролем TOTP з терміном дії в 20 секунд та біометричною автентифікацією та прив’язувати всі акаунти (якщо користувач має два і більше акаунтів) до єдиного біометричного параметра, які пропонується обліковувати в окремому реєстрі біометричних даних. Запропоновані заходи дадуть змогу також запобігати спробам обходу бану через створення нових облікових записів завдяки необхідності автентифікації через біометричні дані (фіксацію обличчя або відбиток пальця як більш унікальний параметр). Для ускладнення отримання зловмисниками НСД до облікових записів користувачів пропонується впровадження політики паролів, згідно якої передбачено відхилення реєстрації надто слабких проти зламу паролів (зокрема, наявних в словниках слів, дати народження, прості числові комбінації тощо) та вимога оновлювати пароль кожні 90 діб, щоб запобігти ризикам компрометації паролю.

Також в ході дослідження було встановлено, що на сайті існують ризики зловживання функціонуванням системи постмодерації як системи модерації за

замовчуванням (з моменту створення акаунту), а саме масової публікації неетичного і невідповідного тематиці сайту контенту. Для запобігання цим ризикам згідно розробленого проєкту системи перевірки на мета-дані пропонується впровадити автоматизовану перевірку зображень на мета-дані, яка полягатиме в розпізнанні на фотографії об’єктів (громадського транспорту різних типів). Коли користувач публікує фотографію, вона спершу проходить перевірку на наявність транспортних засобів на фото, в результаті чого або відхиляється одразу, або проходить модерацію (або постмодерацію, коли перевірка якості фотоматеріалів відбувається уже після моменту публікації, або премодерацію, коли перевірка якості фотоматеріалів проводиться перед публікацією фото), яка завершується одним з трьох варіантів: фотографія або приймається спільнотою користувачів та/або модераторами, або відправляється користувачеві на доопрацювання недоліків, або відхиляється через недостатню якість фотографії.

Окрім цього, встановлено, що на сайті краудсорсингової платформи AllTransUA діє система журналювання даних, яка також потребує вдосконалення. На сайті наразі діє лише журналювання змін флоту БД, де фіксується профіль транспортного засобу (запис в БД) з відповідними йому бортовими та/або державними номерними знаками, дата та час правки, місто/регіон, в БД якого було внесено зміни та власне автор-користувач, який вносив зміни (локальний або загальний редактор БД). Для запобігання зловживання адміністративним ресурсом згідно проєкту було розроблено рекомендації щодо впровадження єдиної об’єднаної системи журналювання та аудиту, згідно якої до уже наявного публічного журналювання флоту БД додати публічно доступне журналювання змін привілеїв користувачам, яка фіксує адміністратора, який змінював привілеї щодо конкретного користувача, власне користувача, щодо якого було внесено зміни в повноваженнях, попередню та поточну посади, а також дату та час внесення правок.

Окрім цього, було також розроблено загальний проєкт системи безпеки сайту AllTransUA, який поєднує в собі функціонально пов’язані проєкти інших ключових і найбільш вразливих функціональних компонентів.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці і правила протипожежної безпеки

Дослідження та розробка проєкту системи безпеки користувачів краудсорсингової платформи AllTransUA відбувалися в аналогічних умовах до тих, в яких працюють офісні працівники. Тому в даному розділі описано охорону праці працівників, що працюють з екранними пристроями, зокрема з стаціонарними та портативними ПК.

Законодавство та нормативні документи, що стосуються охорони праці, впроваджуються та розробляються з ціллю захисту здоров'я та життя працівників і підвищення рівня їхнього добробуту, і стосується також галузі ІТ, оскільки в цій галузі також існують ризики з точки зору гігієни праці та техніки безпеки [15].

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

Охорона праці – це передусім система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, ціллю яких є забезпечення безпеки, охорони праці та працездатності людини впродовж усього процесу праці.

На кожного працівника впливають такі ж фактори, що і в будь-якому офісному приміщенні та будь-якому іншому середовищі – рівень захворюваності, умови, освітлення, оточення, характер праці тощо.

Робочі місця працівників з екранними пристроями мають бути спроектовані так і мати такі розміри, щоб працівники мали простір для зміни робочого положення та рухів.

Для забезпечення безпеки та захисту здоров'я працівників усе випромінювання від екранних пристроїв має бути зведене до гранично допустимого рівня (вплив на людину факторів довкілля – шуму, вібрації, забруднювачів, температури тощо, який не спричиняє соматичних або

психічних розладів, а також змін стану здоров'я, працездатності, поведінки, що виходять за межі пристосувальних реакцій) з погляду безпеки та охорони здоров'я працівників.

Організація робочого місця працівника з екранними пристроями має забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним, антропологічним, психофізіологічним вимогам, а також характеру виконуваних робіт.

Освітлення робочого місця працівника з екранними пристроями має створювати відповідний контраст між екраном і навколишнім середовищем (з урахуванням виду роботи). Мікроклімат виробничих приміщень з робочими місцями працівників з екранними пристроями має підтримуватись на постійному рівні та відповідати вимогам санітарних норм.

Робочий стіл або робоча поверхня повинні бути достатнього розміру та мати поверхню з низькою відбивною здатністю, допускати гнучкість під час розміщення екрана, клавіатури, документів і відповідного устаткування.

Робоче крісло має бути стійким і дозволяти працівнику з екранними пристроями легко рухатися та займати зручне положення. Сидіння має регулюватися по висоті, спинка сидіння – як по висоті, так і по нахилу. Слід передбачати підніжку для тих, кому це необхідно для зручності [15].

Порядок дій у разі виникнення пожежі в освітньому закладі:

1. У разі виникнення пожежі дії працівників закладів та установ мають бути спрямовані на створення безпеки людей, в першу чергу дітей, їх евакуацію та рятування.

2. У випадку виникнення пожежі в закладах та установах з цілодобовим перебуванням дітей необхідно керуватися Порядком спільних дій на випадок виникнення надзвичайних ситуацій та пожеж в організаціях, установах і закладах з цілодобовим перебуванням людей.

3. Працівник закладу та установи, який виявив пожежу або її ознаки (задимлення, запах горіння або тління різних матеріалів, різке підвищення температури в приміщенні тощо), зобов'язаний:

- негайно повідомити про це за телефоном до найближчого пожежно-

рятувального підрозділу (при цьому слід чітко назвати місцезнаходження об’єкта, місце виникнення пожежі, а також свою посаду та прізвище);

- задіяти систему оповіщення людей про пожежу; розпочати самому і залучити інших осіб до евакуації людей з будівлі до безпечного місця згідно з планом евакуації;

- сповістити про пожежу керівника закладу та установи або особу, що його заміщує;

- організувати зустріч пожежно-рятувальних підрозділів, вжити заходів щодо гасіння пожежі наявними в закладі та установі засобами пожежогасіння.

4. Керівник закладу та установи або особа, яка його заміщує, що прибув на місце пожежі, зобов’язаний:

- перевірити, чи повідомлено пожежно-рятувальний підрозділ про виникнення пожежі;

- здійснювати керівництво евакуацією людей та гасінням пожежі до прибуття пожежно-рятувальних підрозділів. У разі загрози для життя людей негайно організувати їх рятування, використовуючи для цього всі наявні сили і засоби;

- організувати перевірку наявності всіх учасників навчально-виховного процесу, евакуйованих з будівлі, за списками і журналами обліку навчальних занять;

- виділити для зустрічі пожежно-рятувальних підрозділів особу, яка добре знає розміщення під’їздних шляхів та вододжерел;

- перевірити включення в роботу СПЗ;

- вилучити з небезпечної зони всіх працівників та інших осіб, не зайнятих евакуацією людей та ліквідацією пожежі;

- у разі потреби викликати до місця пожежі медичну та інші служби;

- припинити всі роботи, не пов’язані з заходами щодо ліквідації пожежі;

- організувати відключення мереж електро- і газопостачання, систем вентиляції та кондиціонування повітря і здійснення інших заходів, що сприяють запобіганню поширенню пожежі;

- організувати евакуацію матеріальних цінностей із небезпечної зони,

визначити місця їх складування і забезпечити в разі потреби їх охорону;

- інформувати керівника пожежно-рятувального підрозділу про наявність людей у будівлі.

5. Під час проведення евакуації та гасіння пожежі необхідно:

- з урахуванням обстановки, що склалася, визначити найбезпечніші евакуаційні шляхи і виходи до безпечної зони у найкоротший строк;

- ліквідувати умови, які сприяють виникненню паніки. З цією метою працівникам закладів та установ не можна залишати дітей без нагляду з моменту виявлення пожежі та до її ліквідації;

- евакуацію людей слід починати з приміщення, у якому виникла пожежа, і суміжних з ним приміщень, яким загрожує небезпека поширення вогню і продуктів горіння. Дітей молодшого віку і хворих слід евакуювати в першу чергу;

- у зимовий час на розсуд осіб, які здійснюють евакуацію, діти старших вікових груп можуть заздалегідь одягтися або взяти теплий одяг із собою, а дітей молодшого віку слід виводити або виносити, загорнувши в ковдри або інші теплі речі;

- ретельно перевірити всі приміщення, щоб унеможливити перебування у небезпечній зоні дітей;

- виставляти пости безпеки на входах у будівлі, щоб унеможливити повернення дітей і працівників до будівлі, де виникла пожежа;

- у разі гасіння слід намагатися у першу чергу забезпечити сприятливі умови для безпечної евакуації людей;

- з метою запобігання поширенню вогню, диму утримуватися від відчинення вікон і дверей, а також від розбивання скла.

Залишаючи приміщення або будівлі, що постраждали від пожежі, потрібно зачинити за собою всі двері і вікна [16].

Під час роботи на стаціонарному або портативному ПК потрібно дотримуватися вимог та інструкції.

1. Щодня перед початком роботи необхідно очищати екранні пристрої від пилу та інших забруднень.

2. Після закінчення роботи екранні пристрої слід відключати від електричної мережі.

3. У разі виникнення аварійної ситуації необхідно негайно відключити екранний пристрій від електричної мережі.

4. Не допускається:

- виконувати технічне обслуговування, ремонт і налагодження екранних пристроїв безпосередньо на робочому місці працівника під час роботи з екранними пристроями;

- відключати захисні пристрої, самочинно проводити зміни у конструкції та складі екранних пристроїв або їх технічне налагодження;

- працювати з екранними пристроями, у яких під час роботи виникають нехарактерні сигнали, нестабільне зображення на екрані та інші несправності.

5. Під час виконання робіт операторського типу, пов’язаних з нервово-емоційним напруженням, у приміщеннях під час роботи з екранними пристроями, на пультах і постах керування технологічними процесами та в інших приміщеннях мають дотримуватися оптимальні умови мікроклімату.

Мінімальні вимоги безпеки до екранних пристроїв передбачають наступні правила:

1. Екранні пристрої не мають бути джерелом ризику для працівників.

2. Усе випромінювання, за винятком видимої частини електромагнітного спектра, має бути зведене до незначного рівня з погляду безпеки і охорони здоров’я працівників.

3. Символи на екранних пристроях мають бути чіткими, відповідного розміру. Між символами і рядками символів має бути належна відстань.

4. Зображення на екрані має бути стабільним, без миготінь або інших видів нестабільності.

5. Яскравість та/або контрастність символів має легко регулюватися працівником під час роботи з екранними пристроями, а також швидко адаптуватися до навколишніх умов.

6. Вибираючи екрани, слід надавати перевагу таким екранам, які легко та вільно повертаються і нахиляються відповідно до потреби працівника.

7. За необхідності може використовуватись окрема підставка або регульований стіл для розміщення екрана.

8. Екран не має відблискувати або відбивати світло, щоб не викликати дискомфорту у працівника під час роботи з екранними пристроями.

9. Вибираючи клавіатуру, слід надавати перевагу такій клавіатурі, яка відкидається і є автономною (відокремленою від екрана), щоб працівник міг вибрати зручну робочу позу й уникнути втоми рук (кисті і верхньої частини руки).

10. Поверхня клавіатури має бути матовою, щоб уникнути віддзеркалювання. Розташування клавіш і самі клавіші мають полегшувати роботу із клавіатурою. Позначення клавіш повинно бути достатньо контрастним і розбірливим.

11. Устаткування, яке входить до робочої станції, не має виділяти надлишкового тепла, що може спричинити незручності працівникам під час роботи з екранними пристроями.

12. Під час розробки, вибору, замовлення та модифікації програмного забезпечення, а також під час розробки завдань, що передбачають використання устаткування з екранними пристроями, роботодавець має керуватися таким програмним забезпеченням, яке відповідає розв’язуваним завданням і є простим у використанні, а де необхідно – адаптованим до рівня знань і досвіду працівника [15].

4.2 Безпека життєдіяльності офісних працівників

Вимоги безпеки під час роботи за ПК

- При включенні/відключенні комп’ютерів, оргтехніки та освітлення в електромережу, братися тільки за ізольовані частини штепселів та штепсельних колодок.

- Дотримувати зазначену в інструкції з експлуатації послідовність включення блоків.

- Щоб уникнути розрядів статичної електрики, не допускається

доторкання до екрана монітора.

- При введенні даних, редагуванні програм, читанні інформації з екрана, безперервна тривалість роботи перед екраном не повинна перевищувати 1 годину з наступними регламентованими перервами по 10 хвилин для відпочинку зору та виконуванню комплексу фізичних вправ, релаксаційної гімнастики й аутогенного тренування [17].

При включеному електроживленні комп'ютерів та оргтехніки:

- не розкривати захисні кожухи й кришки блоків ПК, не робити регулювання й чищення внутрішніх деталей, не змінювати запобіжники;

- не переключати сполучні шнури блоків;

- не змінювати встановлену конфігурацію робочого місця, не переставляти комп'ютери та оргтехніку;

- не робити вологе прибирання поверхонь комп'ютерів, моніторів та оргтехніки (прибирання робити спеціальними серветками);

На робочому місці не палити, не користуватися відкритим вогнем та не зберігати легкозаймисті, вибухонебезпечні і хімічно-активні, що руйнують ізоляцію, речовини.

Дотримуватися чистоти і порядку на місці проведення робіт, обережності при роботі, при пересуванні по приміщенню.

Паління дозволяється тільки у спеціально відведених для цього місцях.

При пересуванні по приміщенню бути уважним і обережним. Особливо обережним слід бути після вологого прибирання.

Вимоги безпеки після закінчення роботи:

- закінчити працюючі програми, закрити всі каталоги, підготувати комп'ютер до вимикання.

- відключити ПК і місцеве електроосвітлення від мережі.

- упорядкувати робоче місце, забрати документи, що використовувалися.

- переконатися у відсутності пожежної небезпеки.

- у разі виявлення пошкоджень та несправностей екранних пристроїв, периферійних пристроїв, засобів оргтехніки, меблів, приладів, електропроводки і інших кабелів, електророзеток, електровимикачів,

світильників, кондиціонерів та іншого обладнання не включати устаткування, не приступати до роботи, повідомити про це керівництво.

Ознаками аварійної ситуації на робочому місці є:

- поява збоїв у роботі ПК, заїдання паперу в принтері, зникнення зображення на екрані монітора;

- коротке замикання, іскріння, появи запаху горіння, підвищене нагрівання корпусу, штепсельних рознімань, сполучних проводів, зниження або зникнення напруги в мережі і т.п.

В аварійній ситуації необхідно:

- роботу припинити, відімкнути від мережі комп'ютери та оргтехніку;

- при загорянні використовувати вуглекислотний або порошковий вогнегасники;

- вжити заходів щодо евакуації людей і наданню першої медичної допомоги постраждалим;

- доповісти керівництву офісу про надзвичайну ситуацію;

- за необхідності викликати швидку допомогу, пожежників.

Якщо виникла ситуація, що може призвести до аварії або нещасного випадку необхідно огородити небезпечну зону і не запускати в неї сторонніх осіб. Якщо є потерпілі, надавати їм першу домедичну допомогу, при необхідності викликати швидку допомогу [17].

Надання першої домедичної допомоги.

- при ураженні електричним струмом: негайно звільнити потерпілого від дії електричного струму, відключивши електроустановку від джерела живлення. При відсутності у потерпілого дихання і пульсу необхідно робити йому штучне дихання і непрямий масаж серця .

- при пораненні: розкрити індивідуальний пакет, накласти стерильний перев'язочний матеріал, що міститься у ньому на рану і зав'язати її бинтом. Особливо важливо застосовувати настойку йоду при забруднених ранах.

- при переломах і вивихах кінцівок: пошкоджену кінцівку укріпити шиною, палицею, картоном.

- при імовірному переломі черепа: прикласти до голови холодний предмет

або зробити холодну примочку.

- при переломі ребер (біль при диханні, кашлю, чиханні, рухах): туго забинтувати груди чи стягнути їх рушником під час видиху.

- при опіках вогнем, парою, гарячими предметами ні в якому разі не можна відривати пузирі (I ступінь опіків – обпечене місце обробити ватою, змоченою етиловим спиртом, II ступінь опіків – обпечене місце обробляють спиртовим, 3%-ним марганцевим розчином, III ступінь опіків - накривають рану стерильною пов’язкою та викликають лікаря).

- при кровотечі: необхідно підняти поранену кінцівку вверх, кровоточиву рану закрити перев’язочним матеріалом, якщо кровотеча зупинилася, то не змінюючи накладеного матеріалу, поверх нього покласти ще одну подушечку з іншого пакета чи кусок вати і забинтувати поранене місце;

- при сильній кровотечі, яку не можна зупинити пов’язкою: застосувати здавлювання кровоносних судин, які живлять поранену область, при допомозі згинання кінцівок в суглобах, а також пальцями, джгутом або закруткою та терміново викликати лікаря [17].

Таким чином, при охороні праці були дотримані вимоги, аналогічні до умов праці офісних працівників та розглянуто техніки безпеки при роботі ПК, а також правила протипожежної безпеки.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи освітнього рівня “Магістр”, присвяченої детальному аналізу функціоналу сайту краудсорсингової платформи AllTransUA та розробки проєкту системи безпеки та захисту користувацьких даних, було проведено ряд досліджень, присвячених тематиці багатофакторної автентифікації, перевірки на мета-дані (розпізнання об’єктів на фото), а також дослідженням в галузі журналювання даних. Важливо зазначити, що дослідження проводилися в умовах відсутності до адміністративного ресурсу, тому метою кваліфікаційної роботи є саме розробка рекомендацій та проєкту системи безпеки.

Аналіз функціональних компонентів транспортного ресурсу AllTransUA (можливість публікації матеріалів, фільтрування контенту, ієрархія ролей, система модерації та скарг, журналювання даних, механізми реєстрації та входу та каналів комунікації) показав, що найбільш вразливими функціональними компонентами є публікація матеріалів, система модерації, журналювання даних та механізми реєстрації і входу.

В ході аналізу джерел, присвячених тематиці багатофакторної автентифікації та політики паролів, було встановлено, що найкращою методикою провадження першої з технологій є впровадження як додаткового фактора автентифікації TOTP (Time-based One Time Password), а також автентифікація через біометричний фактор (сканування обличчя або відбитка пальця як більш унікального фактора автентифікації). Також було встановлено, що для захисту паролів від зламу та отримання хакерами НСД важливо розробити політику паролів, яка передбачатиме правила складності та довжини паролів, а також термін дії паролів задля зменшення ризику їхнього перехоплення зловмисниками.

На сайті також існує ризик публікації невідповідного тематиці сайту контенту, зумовленого наявністю публікації контенту на умовах постмодерації як системи модерації за замовчуванням (з моменту створення облікового запису на сайті). В ході аналізу джерел, присвячених перевірці фото на мета-дані, а саме

розпізнанні об’єктів на фотографії, було встановлено, що найвідомішими зразками перевірки фото за зафіксованими об’єктами на фото є засоби фіксації правил порушень дорожнього руху, які фіксують транспортний засіб разом з реєстраційним державним номером, а також інструмент бот-перевірки reCAPTCHA, який запитує вибір фото, де наявні певні об’єкти на фото (включно і транспортні засоби).

Окрім цього, також в ході аналізу джерел, присвячених тематиці журналювання даних та зловживання привілеями було встановлено, що наявна на AllTransUA система журналювання потребує вдосконалення, а саме впровадження журналювання змін привілеїв, аби зменшити ризики прихованого зловживання адміністративним ресурсом.

На основі досліджень було розроблено проєкти системи безпеки для найбільш уразливих компонентів, а саме: проєкт системи багатофакторної автентифікації та політики паролів (механізми реєстрації та входу), проєкт аналізу фото за мета-даними (система модерації та публікація матеріалів), проєкт вдосконаленої системи журналювання, що передбачає як і журналювання флоту БД, так і журналювання змін привілеїв (повноважень) користувачів (журналювання даних). Окрім цього, було розроблено загальний проєкт системи безпеки, що поєднує в собі функціонально пов’язані проєкти інших ключових і найбільш вразливих функціональних компонентів сайту краудсорсингової транспортної платформи AllTransUA

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Завадський К. С. Розробка політики безпеки, моделей загроз та критеріїв захисту інформаційного ресурсу AllTransUA : робота на здобуття кваліфікаційного ступеня бакалавра : спец. 125 - кібербезпека / наук. кер. О. Р. Оробчук. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. 85 с (Дата звернення: 16.12.2025).

2. Харченко О., Яцишин В. Розробка та керування вимогами до програмного забезпечення на основі моделі якості. Вісник ТДТУ. Тернопіль, 2009. Т. 14. №1. С. 201-207 (Дата звернення: 18.12.2025).

3. Lypa B., Horyn I., Zagorodna N., Tymoshchuk D., Lechachenko T. Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings. 2024. vol. 3896. P. 1-11 (Дата звернення: 18.12.2025).

4. Дудикевич, В., Микитин, Г., Насилевський, В., & Фігурняк, В. (2023). ДО ПИТАННЯ БЕЗПЕЧНОЇ БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ У ВЕБ-ЗАСТОСУНКАХ. Ukrainian Information Security Research Journal, 25(2), 76–82. https://doi.org/10.18372/2410-7840.25.17675 (Дата звернення: 11.12.2025).

5. What Is an Authenticator App & How Does It Work. (2025, 26 вересня). Descope. https://www.descope.com/learn/post/authenticator-app (Дата звернення: 12.12.2025).

6. Українцям дали поради для швидкої перевірки і створення Дія.Підпису. (2023, 15 червня). Судово-юридична газета. https://sud.ua/uk/news/ukraine/ 273340-ukraintsam-dali-sovety-dlya-bystroy-proverki-i-sozdaniya-diyapidpisu (Дата звернення: 12.12.2025).

7. Гадяцька, Ю. О. ПОЛІТИКА ПАРОЛІВ ЯК ОСНОВНА ВИМОГА ЗАХИСТУ ІНФОРМАЦІЇ. MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE VN KARAZIN KHARKIV NATIONAL UNIVERSITY, 478 (Дата звернення: 11.12.2025).

8. Бондаренко, К. О., Гнідунець, В. О., & Крупельницький, Л. В. (2024). Розпізнавання об'єктів на фото та відео (Doctoral dissertation, ВНТУ) (Дата звернення: 13.12.2025).

9. Дуляба, Н. (2021, 18 листопада). Спіймати гонщика: все, що треба знати про камери і штрафи за перевищення швидкості. Львівський портал | Новини Львова. https://portal.lviv.ua/news/2021/11/18/spijmaty-honshchyka-vse-shcho-treba-znaty-pro-kamery-i-shtrafy-za-perevyshchennia-shvydkosti (Дата звернення: 13.12.2025).

10. Bostik, O., Horak, K., & Klecka, J. (2017, June). Bubble CAPTCHA-A Start of the New Direction of Text CAPTCHA Scheme Development. In *Mendel* (Vol. 23, No. 1, pp. 57-64) (Дата звернення: 13.12.2025).

11. SebWeo. (2020, 6 грудня). Що таке Google reCAPTCHA? Як отримати API ключі та встановити Капчу? | SebWeo. https://sebweo.com/scho-take-google-recaptcha-yak-otrimati-api-klyuchi-ta-vstanoviti-kapchu/ (Дата звернення: 13.12.2025)

12. Stanciu, N. (2013). Importance of event log management to ensure information system security. Metalurgia international, 18(2), 144 (Дата звернення: 14.12.2025).

13. El-Zawawy, M. A., & Hamdy, A. (2025). Detection of hidden privilege escalations in android. Automated Software Engineering, 32(2), 68 (Дата звернення: 14.12.2025).

14. Kharchenko A., Bodnarchuk I., Yatcysyn V. The Method for Comparative Evaluation of Software Architecture with Accounting of Trade-offs. American Journal of Information Systems. 2014. Vol. 2, No. 1. P. 20-25. URL: http://pubs.sciepub.com/ajis/2/1/5/ (Дата звернення: 18.12.2025)

15. 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.

16. Lupenko, S., Orobchuk, O., Kateryniuk, I., Kozak, R., & Lypak, H. (2023). Secure information system for Chinese Image medicine knowledge consolidation.

17. Ревнюк, О. А., & Загородна, Н. В. (2024). МЕТОДОЛОГІЯ КІЛЬКІСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ВЕБДОДАТКУ ЕЛЕКТРОННОЇ

КОМЕРЦІЇ НА ЕТАПІ ЕКСПЛУАТАЦІЇ. Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas, (2 (57)), 107-119.

18. Revniuk, O., Zagorodna, N., Kozak, R., & Yavorskyy, B. (2025). Development of an information system for the quantitative assessment of web application security based on the OWASP ASVS standard. Вісник Тернопільського національного технічного університету, 118(2), 56-65.

19. Karpiński, M., Revniuk, O., Tymoshchuk, D., Kozak, R., & Tokkuliyeva, A. (2025). Fuzzy logic system as a component of the web application security information system (short paper). CEUR Workshop Proceedings, Article 4042. http://ceur-ws.org/Vol-4042/short4.pdf

20. Stadnyk, M., & Palamar, A. (2022). Project management features in the cybersecurity area. Вісник Тернопільського національного технічного університету, 106(2), 54-62.

21. Деркач М. В., Хомишин В. Г., Гудзенко В. О. Тестування безпеки вебресурсу на базі інструментів для сканування та виявлення вразливостей. Наукові вісті Далівського університету. 2023. №25.

22. Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями, Наказ Міністерства соціальної політики України № 207 (2018) (Україна). https://zakon.rada.gov.ua/laws/show/z0508-18#Text (Дата звернення: 10.12.2025)

23. Про затвердження Правил пожежної безпеки для навчальних закладів та установ системи освіти України, Наказ Міністерства освіти і науки України № 974 (2016) (Україна). https://zakon.rada.gov.ua/laws/show/z1229-16#Text (Дата звернення: 11.12.2025)

24. Інструкція з охорони праці для офісних працівників. Safety: Безпека та охорона праці. URL: https://safety.org.ua/instruktsiya-z-ohorony-pratsi-dlya-ofisnyh-pratsivnykiv/ (дата звернення: 11.12.2025).

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

УДК 004.056.53
К. Завадський, студент; Р. Козак, к.т.н., доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ЗАХИСТУ КОРИСТУВАЦЬКИХ ДАНИХ НА ОСНОВІ СТРУКТУРОВАНОГО АНАЛІЗУ КРАУДСОРСИНГОВОЇ ПЛАТФОРМИ ALLTRANSUA

UDC 004.056.53
K. Zawadskyi, student; R. Kozak, Ph.D., Assoc. Prof.

METHODS FOR PROTECTING USER DATA BASED ON STRUCTURED ANALYSIS OF THE ALLTRANSUA CROWDSOURCING PLATFORM

Сучасні транспортні краудсорсингові платформи, якими користуються щоденно тисячі та десятки тисяч осіб, потребуть захисту користувацьких даних [1], особливо серед тих, що щодня наповнюють транспортну галерею різними фотографіями відповідних категорій. Адміністрація сайту AllTransUA стикається з спам-потоками контенту, що не відповідає його тематиці, і змушена витрачати більше ресурсів з ліквідації небажаного контенту.

Традиційна система модерації потребує більших людських ресурсів для моніторингу контенту, що завантажується на краудсорсингову платформу AllTransUA і реагування на прецеденти, а наявна система журналювання даних відкриває шлях адміністрації до зловживання своїми повноваженнями. Мета роботи оцінити поточну безпекову ситуацію на сайті AllTransUA, впровадити можливі рішення проблеми ризику обходу блокування акаунтів, публікації спам-контенту та зловживання привілеями з боку адміністрації сайту.

У результаті дослідження було ідентифіковано ризики зламу облікових записів, масової публікації неетичного контенту через недосконалість системи модерації та ризики незаконної зміни привілеїв через недостатній рівень прозорості.

Для пом’якшення ідентифікованих ризиків було запропоновано такі заходи захисту:

- багатофакторна автентифікація – запобігає спробам обходу блокування акаунтів та створенню нових облікових записів, а також запобігає спробам отримання несанкціонованого доступу до акаунту;
- перевірка на метадані, що забезпечує зниження ризику публікації контенту, що не відповідає тематиці ресурсу
- прозоре журналювання змін привілеїв, що забезпечує неможливість адміністраторів приховано зловживати своїми повноваженнями та підвищувати/знижувати привілеї користувачів

Побудова проєкту системи безпеки сайту дає змогу адміністрації розробити статегію подальшого вдосконалення безпекових аспектів сайту AllTransUA та знизить потребу в значних людських ресурсах, а також може надати розуміння, як полегшити процес моніторингу контенту, що завантажується щоденно на сайт.

Література

1. Weiping Pei, Yanina Likhtenshteyn, and Chuan Yue. 2023. A Tale of Two Communities: Privacy of Third Party App Users in Crowdsourcing - The Case of Receipt Transcription. Proc. ACM Hum.-Comput. Interact. 7, CSCW2, Article 253 (October 2023), 43 pages.