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

Прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Комп’ютерно-інтегрованих технологій
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Автоматизована система верифікації при контролі знань в умовах дистанційного навчання

Виконав(ла): студент(ка) 4 курсу, групи КА-41
спеціальності 151 – Автоматизація та комп’ютерно-інтегровані технології
(шифр і назва спеціальності)

Сас Д.В.
(підпис) (прізвище та ініціали)

Керівник Коноваленко І.В.
(підпис) (прізвище та ініціали)
Нормоконтроль Козбур І.Р.
(підпис) (прізвище та ініціали)
Завідувач кафедри Савків В.Б.
(підпис) (прізвище та ініціали)
Рецензент Королюк Р.І.
(підпис) (прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет прикладних інформаційних технологій та електроінженерії
Кафедра автоматизації технологічних процесів і виробництв
Освітній ступінь: бакалавр
(назва)
Спеціальність: 151 – Автоматизація та комп'ютерно-інтегровані технології
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри *доц. Савків В.Б.*
____
«_____» _____ 20___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Сас Денис Володимирович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Автоматизована системи верифікації при контролі знань в умовах дистанційного навчання*

Керівник кваліфікаційної роботи *кандитат техн. наук, доцент Коноваленко І.В.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від « 28 » *травня 2024* року *№4/7-552*

2. Термін подання студентом кваліфікаційної роботи ________________

3. Вихідні дані до кваліфікаційної роботи *вступ, анотація, аналітична частина, проєктна, частина, спеціальна частина, висновок. Робота містить 21 рисунок, 6 таблиць. Обсяг виконаної роботи-64 стр.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналітична частина
2. Проєктна частина
3. Спеціальна частина
4. Безпека життєдіяльності, основи охорони праці

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

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	*Коноваленко І.В.*		
Безпека життєдіяльності,	*Сенчишин В.С.*		
основи хорони праці			

7. Дата видачі завдання *«____» ________2024 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи бакалавра	Термін виконання етапів кваліфікаційної роботи	**Примітка**
1.	*Аналітична частина*	*10.02.2024*	
2.	*Проєктна частина*	*30.04.2024*	
3.	*Спеціальна частина*	*20.05.2024*	
4.	*Безпека життєдіяльності, основи охорони праці*	*01.06.2024*	
5.	*Оформлення графічної частини та пояснювальної*	*15.06.2024*	
	записки		
6.	*Захист кваліфікаційної роботи*	*25.06.2024*	

Студент ________________ *Сас Д.В.*
(підпис) (прізвище та ініціали)

Керівник кваліфікаційної роботи ________________ *Коноваленко І.В.*
(підпис) (прізвище та ініціали)

Анотація

Формування віртуального освітнього середовища закладу освіти вимагає нових рішень, щодо забезпечення якісних показників навчання у ньому і у тому числі при проведенні контролів знань студентів, серед яких важливу роль грають засоби ідентифікації особи через розпізнавання за обличчям, що робить актуальним впровадження таких технологій у сучасні системи управління навчанням.

Метою роботи є створення автоматизованої системи верифікації особи, ефективність якої підтверджувалась б в умовах роботи закладу освіти.

Для досягнення поставленої мети у роботі вирішувались такі **завдання**:

1. Проведення аналізу існуючих рішень для верифікації особи при контролі знань та сформування вимог до проектованої системи.
2. Вибір ефективних алгоритмів виявлення та розпізнавання облич.
3. Розроблення та інтегрування в LMS ATutor автоматизованої системи верифікації особи.
4. Дослідження ефективності роботи системи в реальних умовах контролю знань.

Загальна характеристика роботи: проведено аналіз існуючих на ринку рішень для верифікації особи при контролі знань, сформовано вимоги для цільової системи. Розглянуто основні алгоритми і підходи до виявлення та розпізнавання облич в результаті чого обрано ефективну комбінацію алгоритмів гістограми напрямлених градієнтів (HOG) в поєднанні із методом опорних векторів (SVM) та глибинних згорткових нейронних мереж (CNNs). Спроектовано і реалізовано систему фотофіксації та верифікації особи при контролі знань в LMS ATutor та подано результати дослідження ефективності її роботи.

Ключові слова: фотофіксація, ідентифікація особи, розпізнавання обличчя, алгоритми розпізнавання зображень, точність ідентифікації.

Anotation

The formation of a virtual educational environment for an educational institution requires new solutions to ensure quality learning metrics, including during knowledge assessments of students, where means of identity verification through facial recognition play an important role. This makes the implementation of such technologies in modern learning management systems relevant.

The purpose of the work is to create an automated identity verification system, the effectiveness of which would be confirmed in the working conditions of an educational institution.

To achieve this goal, the following tasks were addressed in the work:

1. Conducting an analysis of existing solutions for identity verification during knowledge assessments and formulating requirements for the designed system.
2. Selecting effective algorithms for facial detection and recognition.
3. Developing and integrating an automated identity verification system into the LMS ATutor.
4. Investigating the effectiveness of the system in real conditions of knowledge control.

General characteristics of the work: an analysis of existing market solutions for identity verification during knowledge assessments was conducted, and requirements for the target system were formulated. The main algorithms and approaches to facial detection and recognition were reviewed, resulting in the selection of an effective combination of histogram of oriented gradients (HOG) algorithms in combination with the support vector machine (SVM) method and deep convolutional neural networks (CNNs). A system for photo capture and identity verification during knowledge assessments in LMS ATutor was designed and implemented, and the results of the effectiveness study were presented.

Keywords: photo capture, identity verification, facial recognition, image recognition algorithms, identification accuracy.

Зміст

Вступ

Еволюція суспільства нашого часу характеризується потужним застосуванням для його блага комп'ютерних технологій, які проникли у всі сфери діяльності людини. Інформатизація освіти є невід'ємною частиною таких процесів. Комп'ютерні технології стають невід'ємною частиною цілісного освітнього процесу, що створює передумови до його трансформації та підвищення ефективності.

У застосуванні інформаційних технологій в освітньому процесі мають місце дві головні тенденції. Перша, це використання їх як засібу навчання та пізнання, друга - як засібу здійснення контролю за навчальною та пізнавальною діяльністю студента, що у своєму поєднанні стають основою для побудови віртуального освітнього середовища для закладу освіти.Як форма контролю ефективності навчання у дедалі більшій мірі використовується тестування знань за допомогою компютера, що стає конкретизованим кроком для запобігання суб'єктивізму в оцінюванні діяльності студента. Інстурменти контролю знань студентів у формі тестування продемонстрували себе як респективний засіб підвищення ефективності управління якістю навчального процесу, незважаючи на наявність як прихильників, так і противників.

Співвідношення між останніми у конкретних випадках перебуває у значній кореляції до якісних показників матеріалу тестів та закладених алгоритмів тестового контролю.

Проте існує інша сторона медалі, противники тестування використовують її як аргумент на свою користь - це нові можливості для недобросовісного проходження тестового контролю знань, насамперед під час дистанційного навчання, коли особи, що проходять контроль не знаходяться у спільному просторі та не перебувають в зоні візуального контролю екзаменатора.

Це вимагає додаткових інструментів і організаційних заходів щодо моніторингу й перегляду перебігу процесу тестування, які б дали достовірність добросовісності проходження тестування для учасників. Найпоширенішими зловживаннями такого роду є недоброчесне використання Інтернету або електронних інструментів в інших вікнах операційної системи або браузера та підручних засобів (посібників, конспектів, цифрових пристроїв тощо) а ще, недоброчесна підміна особи, що проходить тестування.

Тому метою роботи стало розроблення та застосування інструментів контролю активності вікна здачі тесту та запровадження інструментів розпізнавання особи та фотофіксації, реалізованих за допомогою сучасних інформаційних технологій.

Ще однією особливістю вирішення поставленої проблеми є те, що заклади освіти у переважній більшості уже використовують системи управління освітнім контентом, які базуються на веб-технологіях і засоби фотофіксації та розпізнавання повинні мати здатність легкого інтегрування у такі системи та не потребувати значних коштів на впровадження відповідного програмно-апаратного забезпечення й реалізовуватись на штатних у тому числі мобільних платформах користувачів.На основі викладеного вище були сформульовані такі завдання роботи

1. Провести аналіз існуючих рішень для верифікації особи при контролі знань. Сформувати вимоги до проектованої системи.

2. На основі порівняльного аналізу обрати ефективні алгоритми виявлення та розпізнавання облич, які б мали високу швидкодію, не були вимогливими до апаратних ресурсів та характеризувались високою точністю.

3. Розробити автоматизовану систему верифікації особи при контролі знань, яка задовольняла б поставлені вимоги. Інтегрувати її в систему управління навчальним матеріалом ATutor.

4. Дослідити ефективність верифікації особи розробленою системою в реальних умовах контролю знань.

1 Аналітична частина

1.1 Аналіз стану питання

Наразі системи прокторингу, особливо у контексті дистанційного навчання, стають все більш актуальними. Прокторинг - це процес нагляду за учнями або студентами під час екзаменів або інших оцінювальних заходів, зазвичай за допомогою технологій, які виявляють шахрайство чи недопустиму допомогу [1–3]. Ключові аспекти стану питання на сьогоднішній день:

1. Зростання популярності дистанційного навчання: за останні роки спостерігалося значне збільшення популярності дистанційного навчання. Це зумовлено розвитком технологій, зручністю та гнучкістю такого підходу.
2. Потреба в ефективному моніторингу студентів: зі зростанням дистанційного навчання зросла і потреба в ефективному моніторингу активності студентів в момент проходження тестів та інших оцінювальних заходів.
3. Технології прокторингу: різноманітні технології прокторингу, такі як веб-камери, мікрофони, програмне забезпечення для відстеження очей та рухів розвиваються швидкими темпами.
4. Проблеми з приватністю та етикою: використання таких технологій часто викликає питання щодо приватності та етики. Деякі системи прокторингу можуть здаватися нав'язливими, а також породжувати питання щодо справедливості та рівності доступу.
5. Поширення обговорень про альтернативи: у зв'язку з проблемами, пов'язаними з приватністю та етикою, а також з ростом критики щодо ефективності деяких систем прокторингу, відбуваються обговорення щодо альтернативних методів оцінювання, таких як завдання, що спрямовані на визначення реального розуміння матеріалу.

6. Інновації та вдосконалення: компанії, що розробляють програмне забезпечення для прокторингу, продовжують вдосконалювати свої продукти, враховуючи отриманий зворотній зв'язок від користувачів та враховуючи етичні стандарти.

Узагальнюючи, системи прокторингу стають все більш актуальними в контексті зростання популярності дистанційного навчання, але їх впровадження потребує уважного врахування приватності, етики та ефективності.

1.2 Актуальність виконання даної роботи

Актуальність створення систем прокторингу полягає в кількох ключових аспектах:

1. Зростання дистанційного навчання: у зв'язку зі зростанням популярності дистанційного навчання, яке стало необхідним у зв'язку з різними обставинами, включаючи пандемію COVID-19, потреба в ефективному контролі та оцінці знань студентів віддалено збільшилася. Системи прокторингу дозволяють забезпечити цей контроль, зберігаючи доброчесність та об'єктивність оцінювання.

2. Забезпечення дотримання академічної чесності: одним із основних принципів освіти є академічна чесність. Системи прокторингу допомагають уникнути плагіату та інших форм недобросовісного способу отримання знань, що підвищує якість та відповідність отриманої освіти.

3. Використання новітніх технологій: системи прокторингу використовують новітні технології, такі як штучний інтелект та комп'ютерний зір, щоб надати ефективний та точний моніторинг студентів в момент тестування, екзаменів або здачі курсових робіт.

4. Підвищення довіри до дистанційного навчання: застосування систем прокторингу може підвищити довіру до дистанційного навчання як серед

студентів, так і серед освітніх установ та роботодавців, які перевіряють академічні досягнення кандидатів.

Отже, створення систем прокторингу відповідає потребам сучасної освіти, сприяючи забезпеченню чесності та об'єктивності оцінювання студентів у віддалених умовах.

1.3 Методи вирішення поставленої задачі

Завдання на розробку полягає у забезпеченні чесності та об'єктивному оцінюванні в момент дистанційного навчання

1. Використання систем прокторингу: розробка та впровадження систем прокторингу є одним із найефективніших методів контролю за дотриманням академічної чесності. Ці системи можуть включати в себе відео- та аудіомоніторинг за допомогою веб-камер та мікрофонів, виявлення неправомірних дій за допомогою аналізу даних та використання штучного інтелекту.
2. Розвиток програмних засобів для виявлення плагіату: створення та використання програмних засобів задля виявлення плагіату дозволяє ефективно контролювати оригінальність робіт студентів. Ці програмні засоби можуть аналізувати текстовий матеріал та порівнювати його з базою даних, щоб виявити можливі випадки копіювання.
3. Організація змішаного формату оцінювання: використання різних методів оцінювання, таких як письмові завдання, тестування в реальному часі та практичні завдання, може знизити ризик маніпулювання або плагіату. Поєднання декількох методів оцінювання дозволяє отримати більш об'єктивний огляд навичок та знань студентів.
4. Підвищення свідомості та навчання студентів щодо академічної чесності: запровадження курсів чи семінарів щодо академічної чесності

може допомогти усвідомити студентам важливість етичної поведінки в академічному середовищі та наслідки порушень правил [4–6].

Ці методи взаємодоповнюють один одного та спрямовані на забезпечення чесності, об'єктивності та якості освіти у дистанційному форматі. Подальший розвиток та вдосконалення таких методів може сприяти підвищенню довіри до дистанційного навчання та покращенню його результативності.

Використання систем прокторингу:

- Відео- та аудіомоніторинг: системи прокторингу зазвичай включають в себе можливість відео- та аудіомоніторингу, який забезпечує відстеження дій студента в момент тестування чи здачі курсових робіт. Веб-камера та мікрофон можуть використовуватися для запису зображення та звуку зони, де знаходиться студент в момент проходження тесту.
- Використання штучного інтелекту: багато систем прокторингу використовують алгоритми штучного інтелекту для аналізу поведінки студента під час тестування. Ці алгоритми можуть виявляти підозрілі дії, наприклад зміна вікна браузера або використання додаткових програм.
- Відстеження рухів курсора та клавіатурних дій: деякі системи прокторингу можуть відстежувати рухи курсора миші та клавіатурні дії студента під час тестування. Це допомагає виявити підозрілі або несправедливі дії, такі як копіювання та вставляння тексту з інших джерел.
- Аналіз обличчя: деякі системи прокторингу використовують технології розпізнавання обличчя для виявлення підозрілих або несправедливих дій студента в момент проходження тесту.
- Запобігання шахрайству: шляхом комбінування цих методів системи прокторингу дозволяють забезпечити високий рівень контролю та запобігти можливому шахрайству чи несправедливим діям під час тестування.

Загалом, системи прокторингу є важливим інструментом щодо забезпечення чесності та об'єктивності оцінювання у дистанційному навчанні, а їх функціональність постійно вдосконалюється завдяки розвитку технологій штучного інтелекту та комп'ютерного зору.

2 Проєктна частина

2.1 Аналіз існуючих рішень для верифікації особи при контролі знань

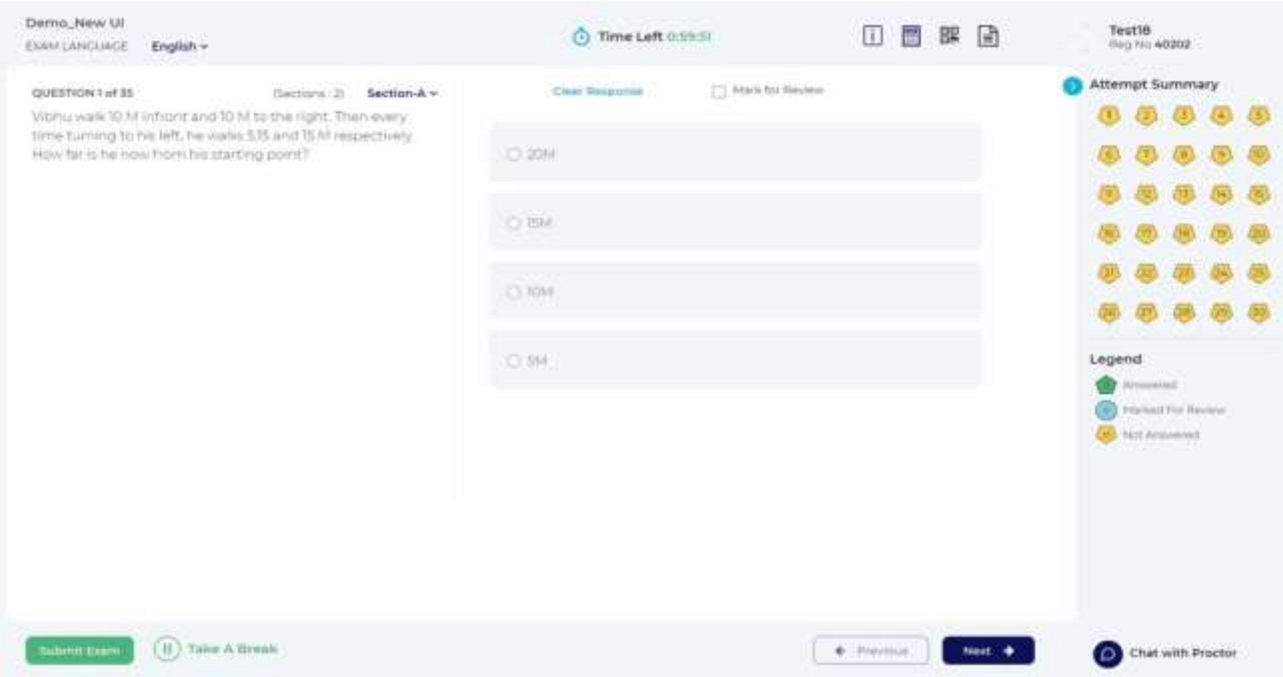
Дистанційні форми навчання з'явилися вже досить давно, але справжній сплеск їхньої популярності був обумовлений режимом самоізоляції членів освітнього процесу через пандемію COVID-19. І якщо проблему з виконанням індивідуальних навчальних завдань вдалося вирішити більш-менш швидко, то віддалений контроль знань засобами тестування досі викликає багато запитань - від безпеки персональних даних до величезної кількості варіантів порушити процедуру перевірки знань.

Одним із перспективних технічних засобів, покликаних вирішити цю проблему, є спеціалізовані системи для верифікації особи при контролі знань тестуванням. Принцип їх роботи такий: користувач через браузер підключається до системи, а та, у свою чергу, в автоматизованому режимі підтверджує особистість, збираючи дані з мікрофона, веб-камери, а також, у деяких випадках, з екрану комп'ютера протягом проходження контролю знань.

При цьому система може в автоматичному режимі приймати рішення про недопуск до тесту чи екзамену, якщо особа, яку розпізнано через веб-камеру не відповідає особі, яка очікувалась, або вона порушила інші умови проходження тестування. Також зібрані дані надаються для перегляду екзаменатору, а той, у свою чергу, ухвалює остаточне рішення. Такі системи, зазвичай, мають можливість інтегруватись із поширеними системами організації навчального матеріалу (Learning management system, LMS), чи системами дистанційного навчання.

У деяких випадках, інтеграція можлива за допомогою модуля, вже створеного розробниками системи, а в інших - за допомогою API, який можна використати й реалізувати інтеграцію самостійно [7, 9–12].

Далі приводяться найуспішніші рішення проблеми верифікації особи при контролі знань в умовах дистанційного навчання, та проаналізовано їх переваги та недоліки.



Vibhu walk 10 M infront and 10 M to the right. Then every time turning to his left, he walks 5,15 and 15 M respectively. How far is he now from his starting point?

○ 20M

○ 15M

○ 10M

○ 5M

Рисунок 2.1 – Проходження контролю знань у ExamOnline

ExamOnline - багатофункційне комерційне рішення для будь-яких видів контролю знань онлайн - іспити та інший контроль знань в закладах освіти, кваліфікаційні іспити за місцем праці, оцінювання кваліфікації працівника, сертифікація, наймання на роботу в компанії тощо. Це платформа, яка реалізує повний спектр функцій від керування заявками до проведення онлайн-іспиту, обробки результатів та генерування звіту з результатами.

Серед переваг: підтримка двох відеопотоків для камер з оглядом 360 градусів; виявлення та розпізнавання обличчя на основі штучного інтелекту; запис звуку з мікрофона; повний звіт із записом дій студента та автоматичною оцінкою доброчесності; виявлення людської мови в аудіопотоці; можливість під'єднати реальну людину-проктора для нагляду за перебігом контролю знань; власний браузер із контролем активності інших програм в операційній системі.

Серед недоліків: рішення комерційне та із закритим вихідним кодом; неможливість вбудувати безпосередньо в систему управління навчальним матеріалом, доступна лише обмежена інтеграція із Moodle; відсутня будь-яка інтеграція із LMS ATutor [13–19]; працює лише у браузері Google Chrome.

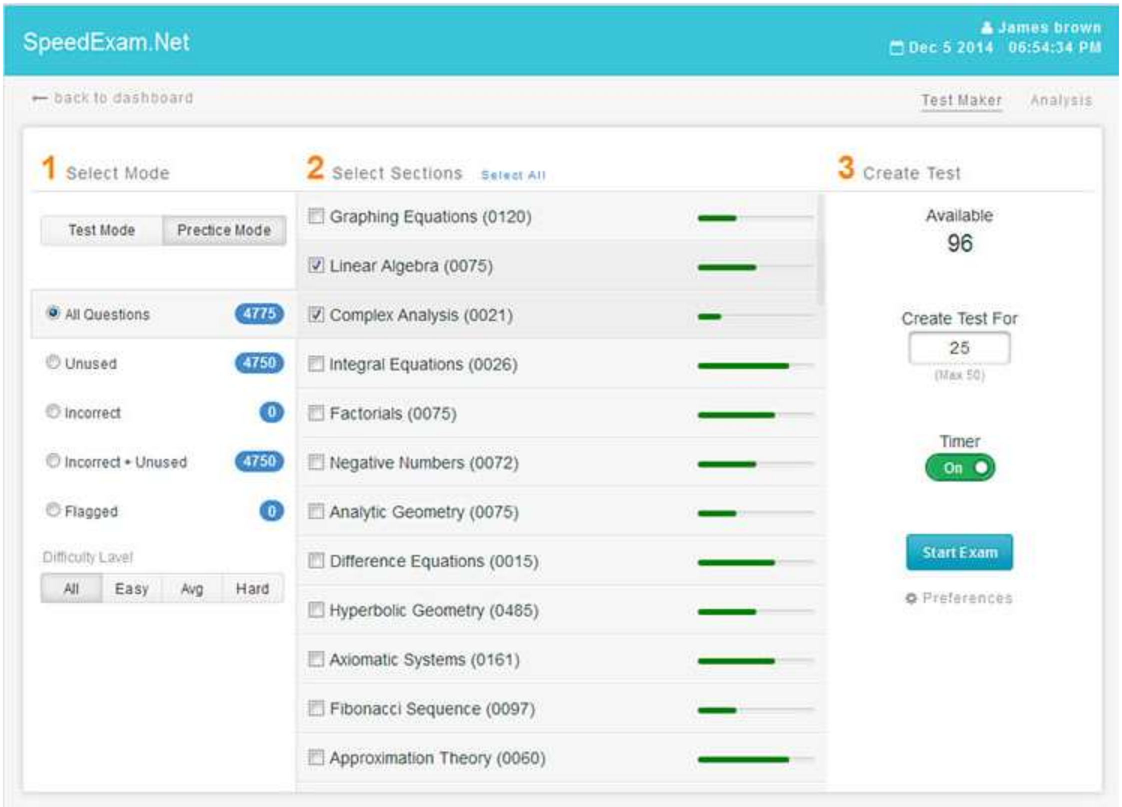
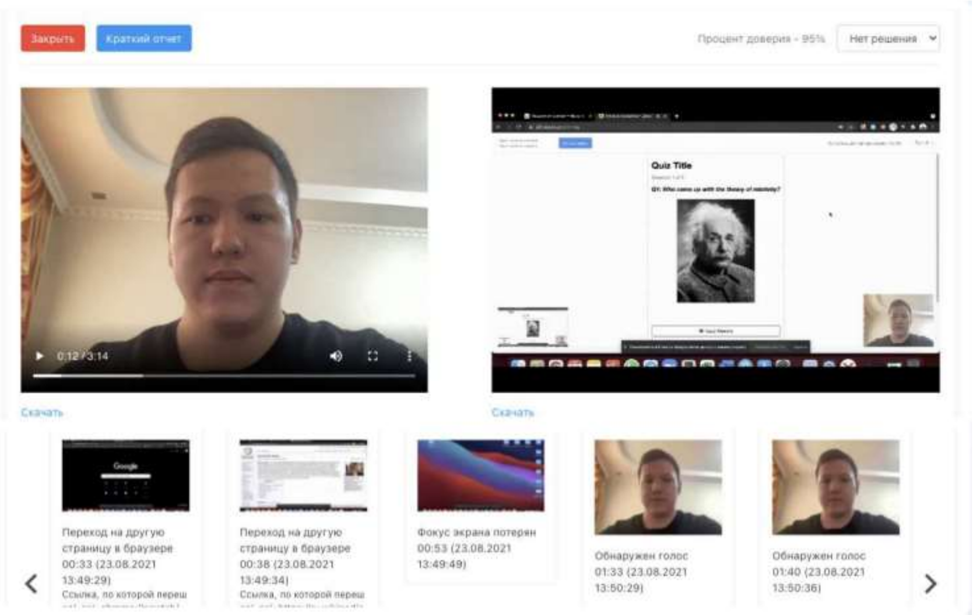


Рисунок 2.2 – Створення тесту у SpeedExam

SpeedExamSpeedExam - універсальне комерційне програмне забезпечення для онлайн-іспитів, яке пропонує декілька розширених функцій, таких як автоматичне оцінювання та миттєві звіти.

Серед переваг: запис екрану; пакетний імпорт тестових запитань із формату Word та Excel.

Недоліки: неможливість працювати безпосередньо вбудованими в LMS інших розробників - це окреме комерційне рішення, яке практично ніяк не інтегрується із LMS і вимагає окремого імпорту банку тестових запитань в цю систему або їх ручного внесення туди.



Переход на другую страницу в браузере 00:33 (23.08.2021 13:49:29) Ссылка, по которой переш

Переход на другую страницу в браузере 00:38 (23.08.2021 13:49:34) Ссылка, по которой переш

Фокус экрана потерян 00:53 (23.08.2021 13:49:49)

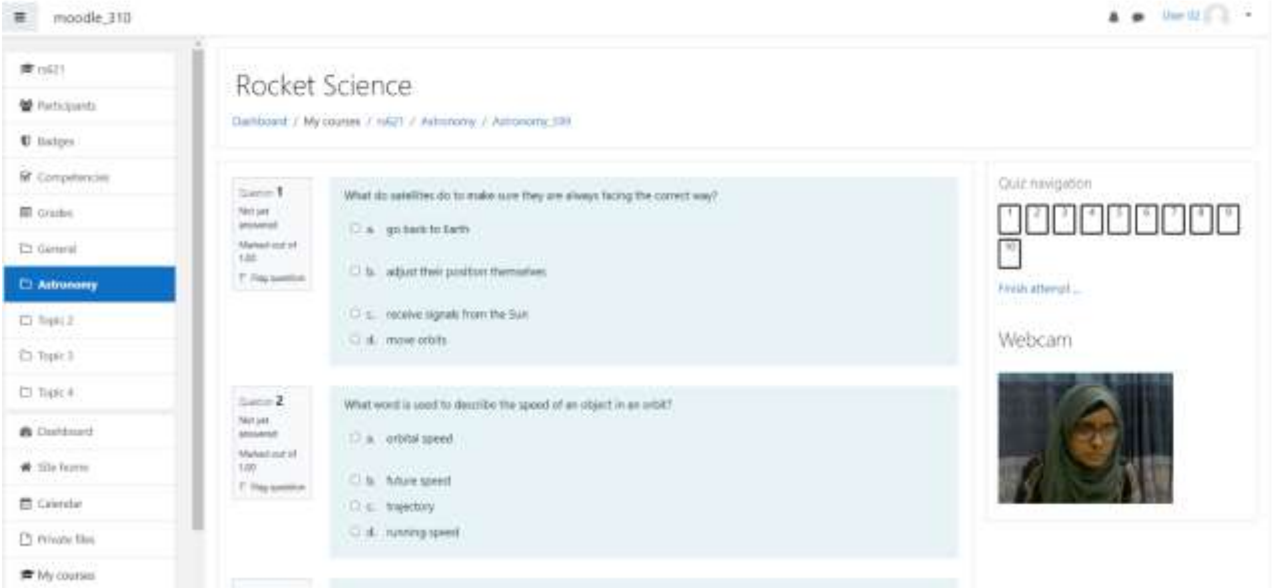
Обнаружен голос 01:33 (23.08.2021 13:50:29)

Обнаружен голос 01:40 (23.08.2021 13:50:36)

Рисунок 2.3 – Захоплення зображення з веб-камери та робочого столу у OESMoodle

OES- система автоматичного прокторингу, представлена казахським розробником. Система повністю контролює камеру, мікрофон, екран студента з використанням технологій ШІ, Computer Vision тощо.

Серед переваг: висока точність розпізнавання облич, фіксація посторонніх осіб, а також шумів та голосів, перевірка наявності декількох екранів, блокування правої кнопки миші, фіксація спроби копіювати або вставити текст, робота зі слабким інтернетом та непотужними ПК [20–24]. Система здатна інтегруватися з такими LMS як Univer, Moodle, Canvas, Indigo, Sirius.



Question 1
Not yet answered
Marked out of 1.00
Flag question

What do satellites do to make sure they are always facing the correct way?

○ a. go back to Earth
○ b. adjust their position themselves
○ c. receive signals from the Sun
○ d. move orbits

Question 2
Not yet answered
Marked out of 1.00
Flag question

What word is used to describe the speed of an object in an orbit?

○ a. orbital speed
○ b. future speed
○ c. trajectory
○ d. running speed

Рисунок 2.4 – Проходження тесту з використанням Moodle Proctoring

Moodle Proctoring - плагін LMS Moodle для верифікації особи при контролі знань, який дозволяє робити фотографії користувача за допомогою веб-камери, щоб визначити, хто намагається пройти тест Moodle. Автоматично знімає зображення кожні 30 секунд (налаштовується) і зберігає його як файл PNG на сервері. Також робить знімки екрана під час тесту. Перед початком тесту, плагін запитує дозволу на доступ до камери та на перегляд екрана. Надавши дозвіл, користувач може побачити своє зображення та розпочати відповідати на запитання тесту. З певною періодичністю знімки з веб-камери та екрану надсилаються на сервер, тому користувач не намагатиметься зробити щось підозріле під час контролю [25–26].

Серед переваг: рішення повністю відкрите (open source), вбудовується в LMS Moodle, завдяки чому працює із наявним банком тестових запитань та налаштованим тестовим рішенням LMS Moodle; API для зовнішнього доступу. Підключивши API Amazon Rekognition або Brainstation Facerecognition є можливість включити автоматичне розпізнавання облич.

Серед недоліків: система не забезпечує автоматичний допуск/недопуск до контролю - для ухвалення рішення потрібна людина; відсутня власна реалізація алгоритмів розпізнавання облич - ця функція покладається на сторонні комерційні API, що вимагатиме додаткових коштів.

Отже, за результатами аналізу відомих існуючих рішень для верифікації особи під час контролю знань можна підвести такі підсумки:

-всі рішення, окрім Moodle Proctoring, не дозволяють повноцінно вбудувати їх у поширені системи електронного навчання (LMS), щоб використовувати вже наявний там банк тестових запитань та наявні вже налаштовані рішення для контролю знань;

-всі рішення окрім Moodle Proctoring є комерційними та із закритим вихідним кодом, що не дає права на модифікацію чи доопрацювання;

-розглянуті технічні рішення не мають можливості інтеграції із LMS ATutor в будь-якому виді;

-жодне із рішень не забезпечує гарантованого високого відсотка (95% і більше) безпомилкового результату.

Це обумовлює потребу проведення подальших пошукових досліджень, з метою вибору, розроблення та впровадження технічного рішення, яке б забезпечувало автоматичну ефективну верифікацію особи при контролі знань у системі тестування LMS закладу освіти на основі використання веб-технологій, високоефективних засобів розпізнавання особи. Важливим є те, щоб технічні рішення такого роду спирались на використання штатного програмно-апаратного забезпечення користувачів, що суттєво мінімізує затрати на їх впровадження в існуючі системи електронного навчання.

2.2 Вибір алгоритмів для виявлення та розпізнавання облич

Виявлення обличчя, що є однією із варіацій загальної задачі виявлення об'єктів, може бути визначене як встановлення того, чи задане зображення містить обличчя, і якщо воно його містить, знайти розташування кожного обличчя.

Виявлення обличчя - це ключове завдання, оскільки воно є необхідною умовою для вирішення інших завдач, таких як локалізація облич розпізнавання облич, аналіз облич, верифікація облич, маркування облич, відстеження (трекінг) облич, розпізнавання емоцій та виразів облич.

Розпізнавання обличчя - це основна задача при ідентифікації або верифікації особистості з використанням її обличчя. Це одна з найважливіших задач комп'ютерного зору з великим комерційним інтересом.

На сьогоднішній день існує декілька десятків комп'ютерних методів виявлення та розпізнавання обличчя. Однак ці методи не дають 100% надійності ідентифікації і разом з цим мають обмеження по продуктивності розпізнавання. Більшість ранніх алгоритмів (до 2012-го року) не змогли забезпечити достатню продуктивність та точність через високу мінливість зображень.

Серед основних викликів і проблем розпізнавання є:

-не завжди задовільна освітленість об'єкту розпізнавання;

-змінні вирази емоцій на обличчях;

-різні типи відтінків шкіри та складний фон;

-варіювання орієнтації та відстані до об'єкта розпізнавання;

-наявність декількох облич на одному зображенні;

-часткове перекриття облич окулярами, елементами одягу, руками, -волоссям, медичними масками тощо;

-недостатня роздільна здатність відеообладнання.

Незважаючи на те, що на сьогоднішній день існує різноманіття методів, можна виділити загальну структуру процесу виявлення та розпізнавання обличчя (див. рис. 1.5).

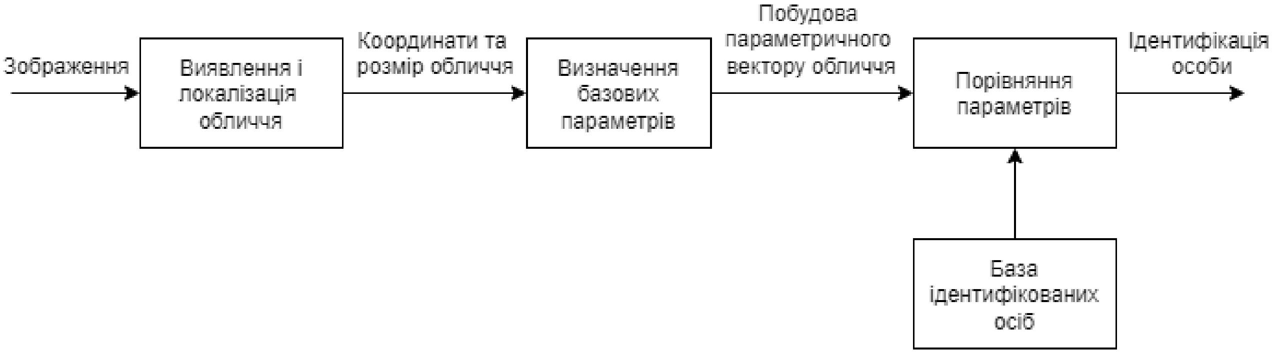


Рисунок 2.5 – Схема процесу обробки зображення обличчя при розпізнаванні

На першому етапі виконується виявлення та локалізація (знаходження координат) обличчя на зображенні. Найкращі результати досягаються в тому випадку, чи у той момент, коли людина дивилась прямо в кадр під час зйомки зображення, однак сучасні алгоритми, також, дозволяють виявляти обличчя в ситуаціях, коли людина не дивиться безпосередньо в камеру (звичайно, у певних межах). Результатом виявлення і локалізації є знайдені координати обличчя(ч) та його(їх) розміри.

На етапі визначення базових параметрів, зображення обличчя вирівнюється та нормалізується (геометрично та за яскравістю), відбувається кодування обличчя в набір базових параметрів, сформований параметричним вектором (масивом). Після цього відбувається саме розпізнавання - порівняння розрахованих параметричних векторів із ідентифікованими, розташованими в базі даних ідентифікованих осіб.

Основною відмінністю всіх розглянутих алгоритмів буде сам механізм виявлення облич та механізм обчислення базових параметрів - транслювання обличчя у параметричний вектор.

До найпоширеніших алгоритмів розпізнавання обличчя можна віднести:

-гнучке порівняння на графах(elastic graph matching);

-метод головних компонент (principal component analysis, PCA);

-алгоритм Віоли-Джонса;

-алгоритм HOG (Histogram of Oriented Gradients) та його комбінування із SVM (Support Vector Machine) класифікатором;

-глибинні згорткові нейронні мережі (Deep Convolutional Neural Networks, Deep CNNs): AlexNet, VGG, ResNet тощо.

Розглянемо найперспективніші з перерахованих методів виявлення та розпізнавання облич у зображеннях, проаналізуємо їх переваги та недоліки і виберемо найоптимальніший для даного проекту. Вимогами до алгоритмів для даного проекту є: точність ідентифікації понад 95%; швидкість розпізнавання до 1 секунди.

Гнучке порівняння на графах. Суть цього методу
полягає в еластичному порівнянні графів, що описують зображення облич. Обличчя представлені у вигляді графів зі зваженими вершинами та ребрами. Під час розпізнавання, один з графів - еталонний - залишається незмінним, а інший змінюється з метою найкращої подібності до першого.

Серед переваг цього методу: відносно хороша точність розпізнавання серед не-ML алгоритмів (може наближатись до 90%); відносна стійкість до зміни ракурсу зйомки обличчя.

Серед недоліків: висока обчислювальна складність унаслідок того, що процедура по черзі виконується з кожним обличчям з бази ідентифікованих осіб; пряма залежність часу роботи від кількості осіб у базі, що за великого обсягу останньої викличе значні затримки.

Метод головних компонент (PCA). Є способом зменшення розмірності даних при втраті мінімальної кількості інформації. Процес обчислення основних компонентів зводиться до обчислення власних векторів та власних значень коваріаційної матриці вхідних даних, або до сингулярного розкладання (SVD) матриці даних. Метод головних компонентів є статистичним і оперує не зображеннями, а векторами в лінійному просторі. У випадках, коли на зображенні присутні значні зміни у рівні освітленості, або виразі обличчя особи, ефективність методу значно знижується.

Серед переваг цього алгоритму можна виділити низькі вимоги до обчислювальної потужності. Однак він має суттєві недоліки: висока чутливість (відносно інших алгоритмів) до освітлення, виразів та ракурсу обличчя; більш жорсткі вимоги до якості зображень порівняно з іншими алгоритмами, через що забезпечується невисока точність розпізнавання (зазвичай, не вище 80-90%).

Алгоритм Віоли-Джонса. Базується на інтегральному представленні зображення по ознаках Хаара, побудові класифікатора на основі алгоритму адаптивного бустингу (AdaBoost) та способі поєднання класифікаторів у каскадну структуру. Цей метод демонструє високу ефективність при вирішенні завдання пошуку об'єктів на зображеннях та у відеопотоках у режимі реального часу. Має низьку ймовірність хибного виявлення обличчя. Дозволяє виявити обличчя при ракурсах під кутом до 30 градусів. Точність ідентифікації може сягати значень понад 90%. Метод був розроблений у 2001 році, має багато реалізацій і широко застосовується на практиці, як простий та ефективний. Алгоритм реалізований також у вільній бібліотеці OpenCV.

Переваги порівняно із алгоритмами гнучкого порівняння графів та PCA: низький відсоток хибних спрацювань;висока швидкість роботи (десятки мілісекунд на сучасних CPU);дещо вища точність;простота реалізації ПЗ (завдяки готовій реалізації у OpenCV).

Алгоритм HOG + SVM класифікатор. Алгоритм гістограми напрямлених градієнтів (HOG) в поєднанні із методом опорних векторів (SVM) може бути використаний для тренування дуже точних класифікаторів об'єктів, в тому числі облич людей - N. Dalal та B. Triggs вперше це продемонстрували у своїй статті Histogram of Oriented Gradients for Human Detection. HOG підраховує кількість певного орієнтування градієнту в локальних ділянках зображення.

Ідея полягає в тому, що розподіл локальної інтенсивності та направленості градієнту описує локальний вигляд та форму об'єкта. Переваги: значно вища точність ніж у каскадів Хаара (метод Віоли-Джонса);стабільніше розпізнавання ніж у каскадів Хаара; хороша швидкість роботи (менше секунди на сучасних CPU).

Недоліки: чутливість до ракурсу обличчя, вимагає фронтального виду; точність поступається глибинним згортковим мережам.Цей алгоритм задовольняє поставлені вимоги, він має достатню точність при все ще достатній швидкості, і може використовуватись в даній системі.

Глибинні згорткові нейронні мережі (Deep CNNs). Глибинні ЗНМ (CNNs) - це тип штучної нейронної мережі (ANN), створений за подобою зорової кори ссавців. Основними компонентами ЗНМ є згорткові фільтри, агрегувальний шар, шар зрізаних лінійних вузлів, повноз'єднаний шар (FC) і шар функції втрат. ЗНМ використовуються у широкому спектрі рішень для виконання завдань розпізнавання об'єктів та дій, виявлення об'єктів, обчислювальної фотографії та обробки природної мови.

Станом на сьогоднішній день саме глибинні ЗНМ досягли видатних успіхів у більшості завдань комп'ютерного зору та домінували у багатьох відомих змаганнях, таких як ImageNet Large Scale Visual Recognition Challenge (ILSVRC). У 2015-му році глибинні згорткові нейронні мережі перевершили людський рівень у класифікації зображень.

Переваги: можна досягнути дуже високої точності розпізнавання (>99%); стійкість до мінливості даних і шумів на вході (ракурс обличчя, освітленість, тіні тощо)

Недолік - через високу обчислювальну складність, вимагає ресурсів графічного процесора (GPU). На основі сказаного вище, для покращення якості роботи розроблюваної системи, актуальним є створення гібридних методів, що поєднували б переваги декількох згаданих алгоритмів. Так комбінування швидшого методу HOG+SVM та повільнішого, але точнішого на CNN (для випадків коли перший незадовільно відпрацює) дозволить створити ефективний детектор. Враховуючи, що саме різновид CNN - залишкові нейронні мережі (ResNet) подолали людський рівень класифікації зображень, а також домінували на змаганнях ImageNet декілька років підряд та демонструють високу точність розпізнавання при достатній швидкості - етап розпізнавання в даному рішенні розумно реалізувати саме на ResNet.

2.3 Аналізування системи управління навчанням

Atutor- це веб-сервіс електронного навчання, розроблений ресурсним центром для груп адаптивних технологій в університеті Торонто, Канада. Це було зроблено на початку 2000-х років для створення зручного та доступного електронного навчального посібника, для задоволення освітніх потреб. Компанія Atutor розробила програму з відкритим кодом, що дозволяє будь-якому користувачеву організації інсталювати без оплати, використовувати та модифікувати цю систему.

Atutor - зручний інструмент для розробки онлайн-курсів та управління навчальним процесом. Через свою гнучкість та адаптивність Atutor використовується багатьма різними установами по всьому світу, в тому числі університети, коледжі, школи та різні організації. Через роки Atutor опинився на міжнародному рівні електронного навчання. Сьогодні він використовується в навчальних закладах організацій на всій земній кулі, підтримує багато мов.

Число користувачів Atutor надалі зростає і демонструє вагоме значення продукту в області електронного навчання. Вивчивши історію та ознайомившись із зростанням більш детально, перейдемо до огляду його функцій. Atutor має великий спектр функцій, завдяки яким ця система чудово працює для вчителів, студентів та системних адміністраторів. По-перше, Atutor легко налаштовується для різних систем електронного навчання. Його можна легко встановити на майже всі веб-сервери, що підтримують PHP, а також MySQL.

Давайте детальніше розглянемо функції, які Atutor надає користувачам.

Можливості для вчителів:

- Створення курсів: вчителі самі створюють курси, які включають різні типи медіа та наповнюють їх вмістом.

- Управління курсом: викладачі можуть налаштовувати параметри курсу, імпортувати або видаляти матеріал, покращувати інформацію та слідкувати за статистикою курсу.

- Оцінка: вчителі встановлюють критерії оцінювання для конкретного тестового завдання та перевіряють їх.

- Інтеракція зі студентами: система вміщає зручні інструменти для спілкування зі студентами, такі як форуми, чати та приватні повідомлення.

Можливості для студентів:

- Перегляд курсу: студенти мають доступ до доступних їм курсів, розділів, можливість читати навчальні матеріали, переглядати відео, переслуховувати аудіофайли та переглядати результати тестів.

- Рейтингова система: учні здобувають оцінки за виконані викладачем завдання та можуть бачити загальний прогрес курсу.

- Інтерактивні елементи: форуми, чат-боти та інші засоби комунікації дозволяють студентам обговорювати матеріали курсу, ставити питання та обмінюватися враженнями та пропозиціями з іншими студентами та спостерігачами.

Персоналізація: можливість налаштування особистого профілю, включаючи зображення та контактну інформацію. Крім того, завдяки відкритому вихідному коду Atutor має змогу розширюватися і змінюватися за допомогою плагінів, адаптуючи систему до конкретних потреб користувачів. Проте, на використання цих корисних і потужних інструментів також варто звертати увагу до питань безпеки. Як і в будь-якій іншій великій системі, Atutor має вразливості, які були включені до популярної бази даних вразливостей CWE.

При огляді кількості та типів вразливостей, виявлених протягом існування Atutor, можна зробити деякі висновки про якість продукту з точки зору безпеки. Хоча наявність вразливостей програмного забезпечення, подібно до Atutor, може видаватися небезпечною за своєю природою, важливо розуміти, що виявлення та усунення цих вразливостей є частиною процесу розробки програмного забезпечення.

Ці кроки свідчать про активний розвиток програми та відповідальне ставлення до безпеки, що привертає увагу розробників та експертів з безпеки. Після вивчення вразливості Atutor, виявленої на веб-сайті CVE Details на рисунку 1.6 можна зробити деякі висновки. Усього було виявлено більше 20 вразливостей різних типів, більшість з яких пов'язані з виконанням коду, переповненням буфера, XSS, CSRF, а також іншими поширеними веб-вразливостями.

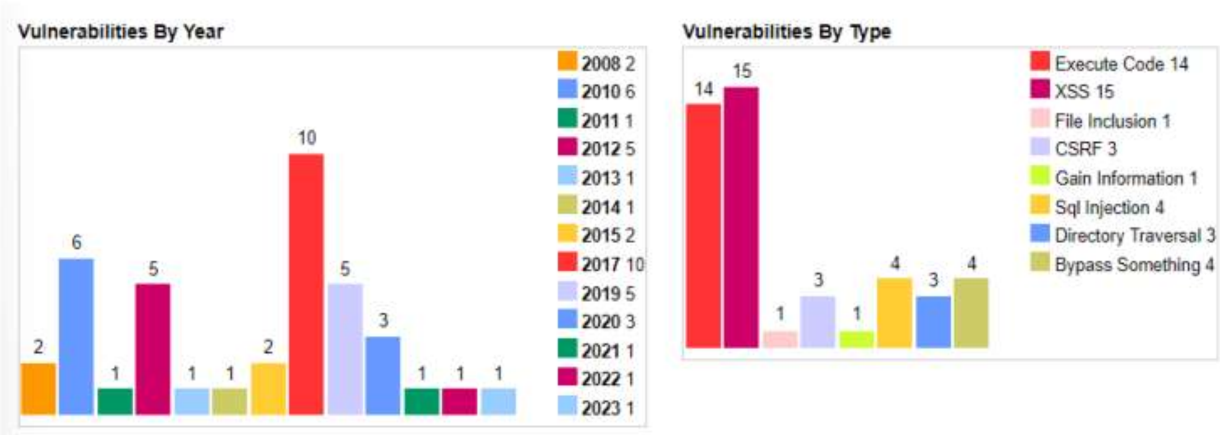


Рисунок 2.6 – Статистика старих виявлених вразливостей

Протягом цього часу деякі вразливості мали серйозний і значний вплив на систему. Проте слід підкреслити, що кількість ідентифікованих вразливостей згодом зменшується, а це свідчить активну роботу розробників над виправленням проблеми. Порівнюючи з іншими аналогічними системами, такими як Moodle Blackboard, Atutor має менше критичних вразливостей. Це свідчить про високоякісний код Atutor та проведення тестів розробниками разом зі спільнотою. Таким чином, на підставі отриманих даних можна зробити висновок, що Atutor, хоча і має деякі вразливості, проте залишається безпечною електронною системою навчання, а його розробники активно працюють над виявленням та усуненням вразливостей. Таке твердження аргументується зменшенням числа виявлених вразливостей в порівнянні з початком. Однак рекомендується інсталювати останню версію програмного забезпечення та завчасно завантажувати найактуальніші пакети безпеки.

2.4 Реалізація LMS Atutor у навчальному закладі ТНТУ

Тернопільський державний технічний університет (ТНТУ) інтенсивно використовує систему електронного навчання Atutor для ведення інноваційного та ефективного навчання. Це підтверджується великою кількістю користувачів і наявністю надійної платформи для управління навчанням. Зокрема, дана система дає змогу університету управляти даними, їх обробкою та захистом.

Крім того, Atutor є гнучкий в плані налаштування навчальних матеріалів відповідно до потреб та вимог дисциплінарного курсу. Atutor поширюється локально в університетах по всьому світу, і сервер підключається до сервера у форматі mpap. Місцеві університети мають повний контроль над своїми системами, включаючи користувачів курсів. Захист даних користувача також забезпечується на більш високому рівні. Однак дані зберігаються в процесі та не передаються третім особам.

Інтеграція з LDAP забезпечує єдину систему аутентифікації та контролю доступу для всіх університетських систем, в тому числі Atutor.

Atutor тісно співпрацює з автоматизованою системою управління "університет". Система широко використовується в студентських спільнотах, освітніх програмах, досягненнях і т.д. Це дуже важливо для функціонування університету, оскільки в ньому зберігаються всі важливі дані, якими володіє університет. Інтеграція системи управління університетом та його викладачів створює додаткові можливості для ефективного управління освітнім процесом. За допомогою вчителів він не тільки автоматично отримує інформацію про зміни в їх освіті, місцезнаходженні, роботі студентів, приймаючих адміністраторів вчителів, але також дозволяє студентам отримувати ту ж інформацію і ресурси для навчання в режимі реального часу.

Веб-сервер nginx признаний завдяки надійності, високій продуктивності та гнучкості у використанні. Це дає змогу успішно обробляти велике число одночасних підключень, що особливо важливо для навчальних закладів, де студенти з викладачами мають одночасний доступ до системи. Atutor відповідає за проведення тестування, побудову курсів, проведення переговорів та тренінгів. Основна частина - це докладний опис функцій вчителя, реалізованих ТНТУ, та їх конкретне використання задля ведення навчального процесу.

Однією з ключових особливостей Atutor є науковий курс, який включає як теоретичні матеріали, так і можливості віртуальної лабораторії. Студенти можуть отримати чітке уявлення про те, як використовувати власне безпечне віртуальне середовище. Це дозволяє глибше зануритися в предмет і здобути практичні навички. Задля зручності користувачів в системі інтегровані такі інструменти, як перевірка, розподіл панелей, електронні записи. Вчителями вони використовуються для оцінки успішності учнів, прийнятті оцінок тощо.
Крім того, в Atutor реалізовані інструменти для комунікації.

Середовище відеоконференцій дозволяє проводити онлайн-конференції, семінари, консультації та спілкуватися в групах. Засоби відеоконференцій в Atutor дають змогу студентам і викладачам контактувати в режимі реального часу за допомогою аудіо та відеотрансляції, а також текстового чату. Викладачі мають змогу проводити заняття в режимі онлайн, на яких вони мають можливість використовувати презентаційні матеріали з використанням таких інструментів, як малювання, виділення найголовнішого на слайдах та вести дискусії зі студентами. Можливість перегляду екрана з окремою програмою браузера дозволяє користувачам ефективно переглядати навчальні матеріали та процеси.

За допомогою YouTube можна переглядати відео, що дає змогу заняттю стати "живішим" та цікавими. Слід підкреслити, що викладачі можуть робити запис відеоуроків та інтегрувати ці відео у матеріали курсу. Таким чином, студенти можуть подивитися відео після уроку, щоб краще засвоїти матеріал. Студенти-учасники можуть переглядати дослідницькі програми та розповсюджувати їх по центру системи. Це в свою чергу робить процес планування та організації навчання зручнішим та ефективнішим. Atutor має інструменти для моніторингу якості електронного навчання та вивчення прогресу онлайн-занять. Вчителі можуть відстежувати виконання завдань студентами, переглядати успішність, що дозволяє своєчасно вирішувати низку питань.

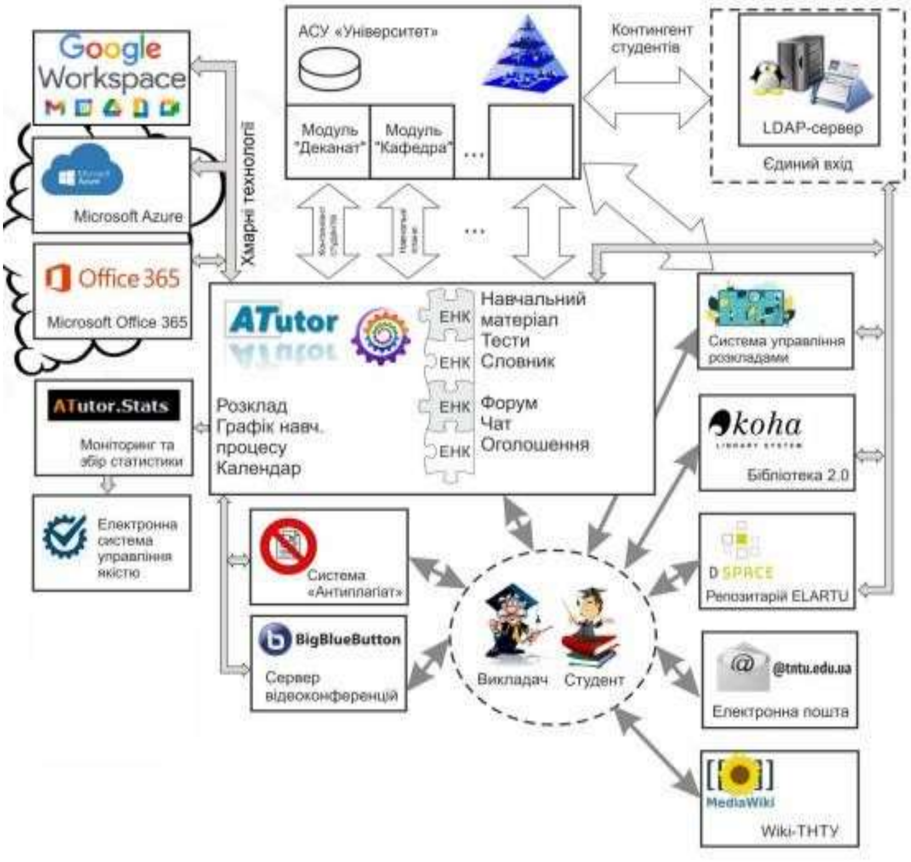


Рисунок 2.7 – Структура освітнього середовища ТНТУ

2.5 Опис структури та реалізації розробленої системи

Розроблене рішення фотофіксації та автоматичної верифікації особи технічно реалізоване у вигляді групи сервісів, які взаємодіють між собою, використовуючи REST API та інтеграції в систему керування навчальним матеріалом ATutor (рис. 2.8).

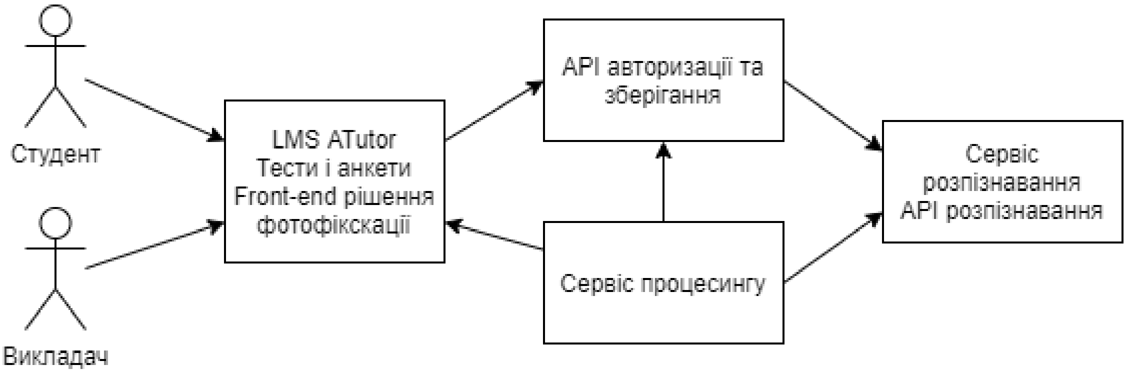
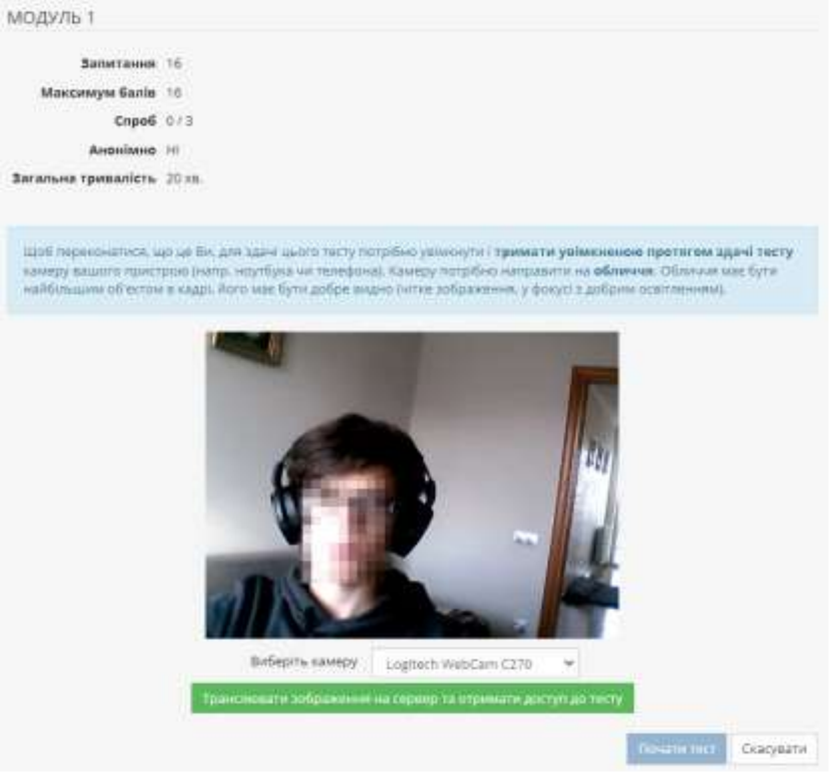


Рисунок 2.8 – Схема архітектури розробленого рішення

Front-end частина рішення тісно інтегрована із модулем "Тести і анкети" LMS ATutor та реалізована на мовах JavaScript, PHP, використовуючи бібліотеки jQuery, Twitter Bootstrap. Взаємодія із камерою студента реалізована, використовуючи Media Capture and Streams API, який підтримується більшістю сучасних браузерів. Рисунок 1.9 Вікно вибору відеокамери і надання дозволу на трансляціюПеред початком тесту студенту потрібно вибрати і надати доступ до пристрою камери та погодитись із надсиланням кадрів із камери на сервер.



МОДУЛЬ 1

Запитання 16
Максимум балів 16
Спроб 0 / 3
Анонімно Ні
Загальна тривалість 20 хв.

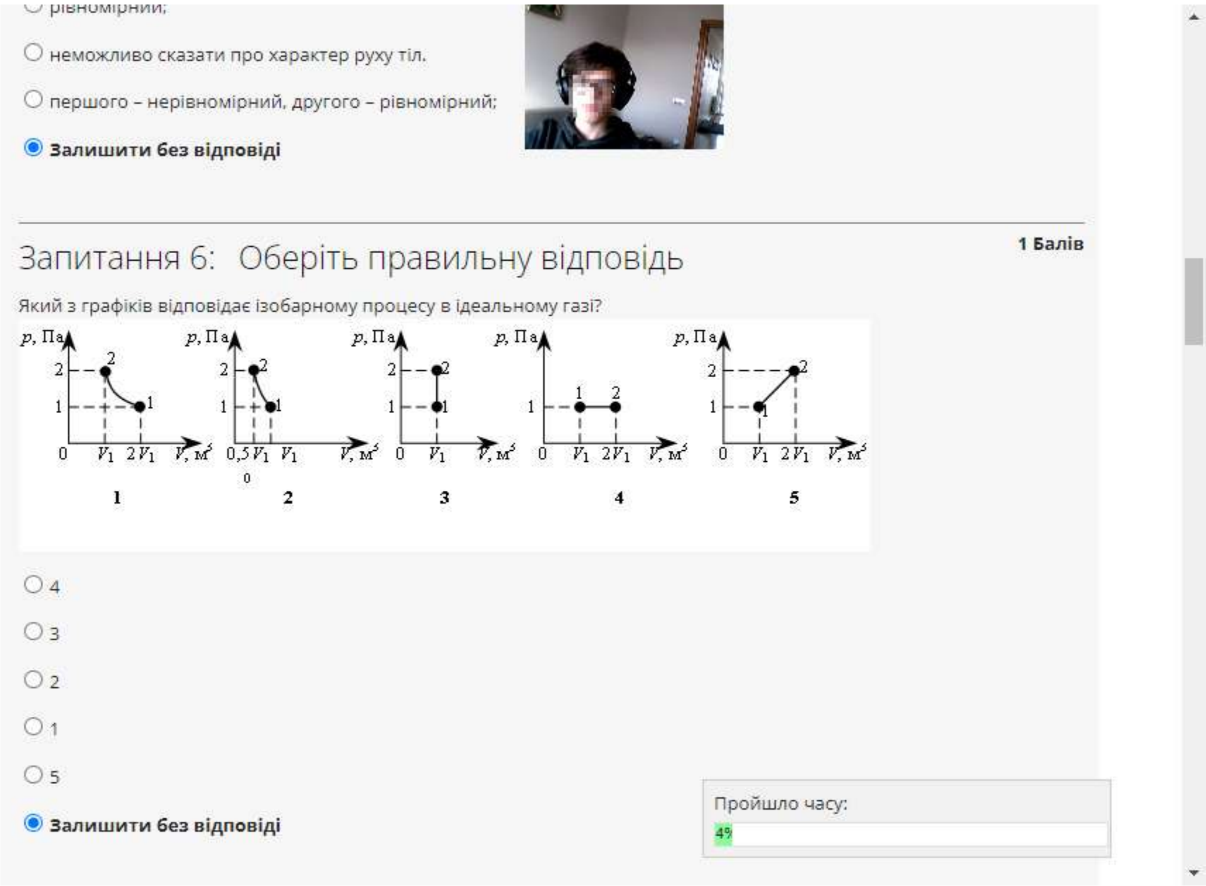
Щоб переконатися, що це Ви, для здачі цього тесту потрібно увімкнути і **тримати увімкненою протягом здачі тесту** камеру вашого пристрою (напр. ноутбука чи телефона). Камеру потрібно направити на **обличчя**. Обличчя має бути найбільшим об'єктом в кадрі, його має бути добре видно (чітке зображення, у фокусі з добрим освітленням).

Виберіть камеру: Logitech WebCam C270

Рисунок 2.9 – Вікно вибору відеокамери і надання дозволу на трансляцію

Кадри проходять авторизацію, використовуючи API авторизації, який видає токен доступу до тесту, отримавши його (і тільки в такому разі), студент зможе почати проходження. Під час проходження студент бачить своє зображення (із кадру камери) у віджеті закріпленому зверху вікна із тестовим проходженням і може коректувати, якщо обличчя вийшло з кадру, або відбулись інші зміни, які унеможливили його розпізнавання.

Під час проходження, кадри з певною періодичністю надсилаються на сервер, використовуючи API авторизації і зберігання, яке записує зображення на диск у форматі jpeg для подальшої обробки. API авторизації та зберігання має два основні ресурси: /auth та /frame.



○ рівномірний;

○ неможливо сказати про характер руху тіл.

○ першого – нерівномірний, другого – рівномірний;

● **Залишити без відповіді**

Запитання 6: Оберіть правильну відповідь

1 Балів

Який з графіків відповідає ізобарному процесу в ідеальному газі?

○ 4

○ 3

○ 2

○ 1

○ 5

● **Залишити без відповіді**

Пройшло часу:

4%

Рисунок 2.10 – Вікно тестового проходження із віджетом кадрів камери

Ресурс /auth авторизує студента для проходження тестового контролю, використовуючи для цього кадр із камери. Ресурс /frame приймає і зберігає кадри із камери у сховище на сервері.

2.6 Дослідження ефективності верифікації особи розробленою системою

Розроблена система була введена в дію та випробована в Тернопільському національному технічному університеті ім. І. Пулюя, також працює і в даний час. Протягом роботи системи зібрано достатньо репрезентативну вибірку даних (на момент написання цієї роботи 1831 студентів здійснили 12499 тестових проходжень), що дозволяє точно оцінити основні статистичні метрики її ефективності. Методика визначення цих метрик включала наступні кроки:

1. Із загальної множини результатів тестувань випадковим чином обирали 200 проходжень.

2. Кожне з обраних проходжень переглядали вручну, визначаючи кількість помилкових відмов, помилкових підтверджень, дійсних відмов та дійсних підтверджень.

3. На основі цих даних обчислювали основні метрики ефективності системи (наприклад, точність, рівень хибних відмов, рівень хибних підтверджень тощо).

Первинні результати аналізу вибірки наведені у таблиці:

Таблиця 2.1 – Результати аналізу вибірки

Позначення	Опис	Значення
TA	кількість дійсних підтверджень	187
TR	кількість дійсних відмов	2
FA	кількість помилкових підтверджень	3

FR	кількість помилкових відмов	8
Разом		200

Одними з найважливіших метрик оцінки якості та ефективності роботи розпізнавальних систем є FAR (False Acceptance Rate - рівень хибних підтверджень) та FRR (False Reject Rate - рівень хибних відмов). FRR - це ймовірність того, що система відмовить у автентифікації справжньому користувачу. FRR розраховується так:

$$FRR = \frac{FR}{N} \times 100\% = \frac{8}{200} \times 100\% = 4\%$$

N- загальна кількість спрацювань.

FAR - це ймовірність того, що система помилково автентифікує неправильного користувача. FAR розраховується так:

$$FAR = \frac{FA}{N} \times 100\% = \frac{3}{200} \times 100\% = 1{,}5\%$$

Типові значення для якісних 2D систем розпізнавання обличчя становлять 2,5% для FRR і 0,1% для FAR. У цьому випадку дещо вищі значення пояснюються значною кількістю тестових проходжень при незадовільних умовах освітлення обличчя.

Іншою важливою метрикою є точність (Precision), яка показує, скільки із підтверджень виявилися дійсно правдивими:

$$\text{Precision} = \frac{\text{TA}}{\text{TA} + \text{FA}} \times 100\% = \frac{187}{187 + 3} \times 100\% = 98{,}4\%$$

Точність використаної моделі ResNet-29 у тесті Labeled Faces in the Wild становить 99,38%. Точність розробленої системи виявилася дещо нижчою, але на етапі розробки це є цілком задовільним результатом. Подальше підвищення точності роботи системи можна забезпечити введенням в алгоритм її роботи попередньої верифікації наявності обличчя у кадрі та оцінювання якості освітлення з наданням рекомендацій щодо усунення недоліків перед початком тестування.

2.7 Огляд системи захисту Atutor

В системі управління навчанням Atutor використовується безліч принципів і методів, створених з метою захисту інформації користувачів:

1. Фільтрація вводу: це важливий спосіб захисту інформації, орієнтований на обробку та перевірку даних, що ввів користувач.

Мета - виявити, видалити або змінити шкідливий вміст, який може пошкодити систему або спричинити збої в роботі. У системі Atutor фільтрація даних використовується задля забезпечення безпеки даних, які ввели користувачі. Це вміщає в себе перевірення даних, введених за допомогою веб-форм, URL-адрес та інтерфейсів.

Фільтрація вхідних даних є ключовим елементом захисту вихідних даних, включаючи об'єкти даних SQL та XSS, які можна використовувати для редагування системних сценаріїв за допомогою вхідних даних. Однак, оскільки цей захист не може гарантувати стовідсотковий захист, важливо зазначити, що фільтрацію можна використовувати в поєднанні з іншими стратегіями захисту для забезпечення максимальної безпеки.

2. Захист екрану за допомогою CSRF: ще один важливий елемент системи безпеки Atutor. Ці атаки зазвичай використовуються, якщо користувач вже пройшов автентифікацію на сайті. Якщо користувач натискає шкідливе посилання або відкриває шкідливий веб-сайт, браузер використовує сеанс потокової передачі для доступу до певного веб-сайту. Atutor виконує ці атаки за допомогою методу CSRF. Кожен запит, до якого ви вносите зміни, повинен містити маркер, створений сервером і пов'язаний із сеансом користувача.

Цей маркер перевіряється, коли сервер отримує запит на зміну. Якщо маркер відсутній або не відповідає на маркер у сеансі, то запит відхиляється. Цей підхід дуже ефективний для захисту від міжсайтового підтвердження запиту (CSRF), оскільки зловмисникам важко отримати доступ до багатьох маркерів. Таким чином, Atutor захищає користувача від можливих атак з перемиканням перехресних запитів.

3. Управління сеансами: управління сеансами є важливим компонентом безпеки на будь-якій веб-платформі, і Atutor тут не є винятком. Веб-сеанс створюється, коли користувач проходить аутентифікацію на сайті, і використовується для відстеження стану користувача в різних запитах. Це дозволяє серверу ідентифікувати користувача і запам'ятовувати його дії. Atutor ідентифікатори сеансів регулярно оновлюються, щоб запобігти блокуванню, а тайм-аути бездіяльності встановлюються для автоматичного видалення старих сеансів. Це важливий захід безпеки, який допомагає зменшити ризик несанкціонованого доступу до облікових записів користувачів та пов'язаних з ними даних. Наприклад, якщо зловмисник намагається скопіювати ідентифікатор сеансу, механізм оновлення може вимкнути його, запобігаючи шкідливому використанню.

4. Хеш пароля: це процес перетворення виводу (в даному випадку пароля) в неоригінальний набір символів фіксованої довжини, незалежно від розміру виводу.

Хеш-функції розроблені таким чином, що невеликі зміни у вхідних даних призводять до абсолютно різних хеш-значень. Atutor використовує цей метод задля безпечного зберігання паролів користувачів. Коли користувач вводить пароль, він перетворюється на хеш-значення і зберігається в базі даних. Пароль, введений під час аутентифікації, знову перетворюється на хеш, і це значення порівнюється з хешем, що зберігається в базі даних.

Цей метод ефективний, оскільки фактичний пароль не зберігається, і зловмисник не може використовувати його безпосередньо, навіть у разі витоку бази даних. Однак слід використовувати найновіші і надійні хеш-функції, які важко зламати. Atutor усвідомлює цю потребу і використовує відповідні алгоритми для забезпечення максимальної безпеки. Atutor використовує модель доступу на основі ролей для надання різних рівнів доступу до системних ресурсів та функцій залежно від ролі користувача. Наприклад, студенти мають доступ до матеріалів курсу, але не можуть їх змінювати, а вчителі мають право редагувати ці матеріали. Цей метод захищає від неналежного або несанкціонованого доступу до інформації та функцій. Це також сприяє збалансованому розподілу прав та обов'язків, щоб кожен користувач мав доступ лише до ресурсів, необхідних йому для виконання своєї ролі.

5. TLS: безпека транспортного рівня (TLS) - це криптографічний протокол, який забезпечує безпечне з'єднання між двома сторонами, як правило, між клієнтом (користувачем) та сервером. TLS працює, створюючи зашифрований канал, по якому передаються дані, забезпечуючи конфіденційність та цілісність даних під час передачі. Atutor активно використовує TLS для захисту даних користувачів під час комунікації між користувачем та сервером. Наприклад, коли користувач вводить свої облікові дані для входу, TLS гарантує, що жоден зловмисник не зможе прочитати або змінити ці дані під час передачі.

Цей тип захисту особливо важливий у сучасному цифровому світі, де зловмисники постійно шукають нові способи перехоплення та використання чужих даних. TLS вважається ефективним і надійним методом захисту і став стандартом для багатьох онлайн-систем, включаючи Atutor. Завдяки використанню TLS користувачі Atutor можуть бути впевнені в безпеці своїх даних при взаємодії з системою.

6. Функція аудиту: це процес відстеження та реєстрації операцій, що виконуються в системі. Вони використовуються для виявлення шахрайських дій, аналізу безпеки та виявлення можливих недоліків. Atutor має вбудовані можливості аудиту, які дозволяють адміністраторам відстежувати активність користувачів. Можна побачити, хто виконав певну дію, коли вона була виконана, та інші відповідні деталі. Це корисно при виявленні розслідування інцидентів, пов'язаних з безпекою, або

підтримка загального дотримання правил і стандартів безпеки. Ця функція важлива для запобігання та виявлення шкідливих дій у системі. Якщо адміністратори виявляють підозрілі дії, такі як незвично велика кількість вхідних запитів або спроби доступу до ресурсів, вони можуть відповісти, наприклад, змінити параметри безпеки, змінити паролі користувачів або повністю заблокувати користувачів. Загалом, функція аудиту є важливим інструментом для забезпечення безпеки Atutor. Вона може допомогти вчасно виявити зловмисників та запобігти можливим порушенням безпеки, що робить її високоефективним методом захисту.

7. Обмеження кількості вхідних запитів: це важлива частина стратегії захисту, спрямованої на запобігання атак типу DoS (збоїв в обслуговуванні). DoS-атака вимагає надсилання великої кількості запитів на сервер, щоб перевантажити сервер і перешкодити його нормальному функціонуванню. Основне завдання brute force полягає в тому, щоб дозволити розшифровку паролів шляхом введення комбінацій. Atutor використовує обмеження кількості вхідних запитів для протидії цим типам атак. Коли система виявляє значну кількість запитів від користувача або IP-адреси протягом короткого часу, вона може тимчасово заблокувати додаткові запити від цього користувача або IP-адреси.

Цей метод також ефективний для запобігання перевантаженню сервера шляхом блокування доступу до облікових записів користувачів. Це впливає на можливість розробки та використання автоматизованих сценаріїв для надсилання паролів або повідомлень для перевірки стабільності та безпеки сервера, команди та системних загроз.

Система безпеки Atutor включає в себе різні стратегії та методи, які працюють у спільноті для забезпечення безпеки даних користувачів, управління сеансами, хешування паролів, протокол TLS, обмеження кількості вхідних запитів, функцію аудиту, фільтрацію вхідних даних. Ці компоненти створюють потужний бар'єр проти більшості загроз безпеці, що виникають в онлайн-освіті. Система не тільки активно виконує атаки, але й використовує інструменти відстеження, які допомагають виявити та нейтралізувати потенційні проблеми. Ці елементи, взяті разом, демонструють високий рівень захисту, пропонований Atutor, і гарантують безпечне для користувача середовище навчання.

2.7.1 Політика інформаційної безпеки Atutor

Політика інформаційної безпеки- це офіційний документ, який визначає правила та процедури для управління, захисту та розподілу інформаційних ресурсів організації. Однією з ключових частин цієї політики є розділ, що стосується маркування критичної інформації. Цей процес визначається ідентифікацією та визначенням рівнів важливості або чутливості даних. Це необхідно для того, щоб організація знала, які саме дані потрібно наділити найвищим рівнем захисту. За відсутності відповідного маркування організація може зіткнутися з проблемами надмірного або недостатнього захисту своїх даних.

Політика також повинна визначати поріг критичності впливу вразливостей на цю інформацію. Це рівень впливу потенційних загроз, який загрожує конфіденційності, цілісності або доступності важливих даних, який є неприйнятним.

Під час визначення порогу критичності враховуються кілька факторів, включаючи значення інформації для організації. Наприклад, для корпоративних секретів або персональних даних клієнта поріг критичності буде дуже низьким. Якщо вразливість перевищує цей поріг, то організація має здійснити заходи для її усунення або зменшення її впливу. Це характеризується оновленням програмного забезпечення, зміною конфігурацій або впровадження нового процесу управління ризиками. Використання порогу критичності впливу є вагомим елементом управління ризиками інформаційної безпеки.

Це допомагає організаціям своєчасно виявляти та деактивізовувати найсерйозніші вразливості, забезпечуючи безперервність роботи та захист даних. У документації Atutor не було знайдено розділу, присвяченого маркуванню критичної інформації. Хоча деякі частини документації згадують важливі дані, вони не містять чітких інструкцій щодо їх маркування чи класифікації. Відсутність зрозумілого маркування критичної інформації ускладнює усвідомлення, як Atutor ідентифіковує та захищає свої найважливіші інформаційні активи, а також проводить оцінку ризиків, пов'язаних з потенційними вразливостями.

2.7.2 Прицнипи визначення захищеності веб-ресурсів

В цифровому середовищі сьогодення забезпечення захисту веб-ресурсів є критично важливим для успішної діяльності будь-якої організації. Існує безліч методів і стратегій, які допомагають оцінювати та підтримувати високий рівень безпеки веб-ресурсів.

Цими методами користуються не лише великі корпорації, але й малі підприємства, некомерційні організації та окремі користувачі. Постійний ріст кількості кібератак і еволюція загроз роблять регулярну оцінку безпеки необхідною процедурою. Такі перевірки зазвичай включають щорічний аудит, що допомагає ідентифікувати потенційні вразливості та покращити методи з інформаційної безпеки. Завдяки сучасним методам оцінки захищеності компанії спроможні забезпечити безпеку своїх веб-ресурсів, захищаючи свої дані, активи та, найважливіше, довіру своїх користувачів. Ось деякі ключові методи, які використовуються для оцінки рівня захищеності веб-ресурсів:

- Аудит безпеки: це деталізований аналіз політики безпеки, процедур та контролю, які застосовуються до веб-ресурсу. Систематична оцінка дає змогу ідентифікувати потенційні вразливості, ризики та недопрацювання в інформаційній безпеці.

Основною метою аудиту є забезпечення захисту важливих активів, включаючи дані та технології. Аудит допомагає впевнитися, що заходи щодо безпеки впроваджені правильно та ефективно, а всі ризики належно управляються. Переваги аудиту включають можливість виявлення вразливостей, перевірку дотримання нормативних вимог і надання рекомендацій щодо покращення безпеки.

Проте, аудит може вимагати значних витрат часу і ресурсів, а його результати можуть бути складними для розуміння неспеціалістами. Крім того, аудит представляє собою "моментний знімок" стану безпеки і не гарантує захисту від можливих загроз. Попри ці недоліки, аудит безпеки є важливим для управління інформаційною безпекою та підтримання належного рівня захисту.

- Тестування на проникнення (Penetration Testing): метод оцінювання безпеки веб-ресурсу методом спроби його "злому" або "проникнення". Метою є імітація дій потенційного зловмисника для виявлення та виправлення вразливостей до їх експлуатації. Цей метод може включати соціальну інженерію, використання відомих вразливостей та фазінг (введення даних навмання для виявлення вразливостей). Головна перевага тестування на проникнення - можливість побачити реальні наслідки вразливостей та провести оцінку ефективності існуючих систем захисту. Недоліками є висока вартість, часозатратність і необхідність високого рівня експертизи. Результати тестування відображають стан безпеки в певний момент і можуть ігнорувати майбутні загрози.

-Сканування вразливостей: це автоматизований процес пошуку та виявлення можливих слабких місць у системах і мережах. Спеціалізоване програмне забезпечення аналізує різноманітні аспекти системи, в тому числі програмне забезпечення, налаштування та версії патчів. Основна мета - виявити та усунути вразливості до їх експлуатації зловмисниками. В нашому цифровому середовищі, забезпечення захисту веб-ресурсів стає критично важливим аспектом для успіху будь-якої організації.

Існують різноманітні методи та підходи для оцінки та забезпечення безпеки веб-ресурсів, які користуються популярністю не лише серед великих компаній, але й серед малих бізнесів, неприбуткових організацій та окремих користувачів. Зі зростанням кількості кібератак і постійними змінами у загрозах, регулярна перевірка безпеки стає невід'ємною складовою процесу. Ці перевірки часто включають щорічні аудити, спрямовані на виявлення вразливостей та покращення заходів безпеки. Використовуючи сучасні методи оцінки безпеки, організації можуть гарантувати захист своїх веб-ресурсів, що є ключовим для збереження даних, активів та довіри користувачів

-Перегляд коду: це процес детального аналізу вихідного коду програми для виявлення потенційних проблем та вразливостей. Він включає пошук небезпечних функцій, недостатніх перевірок безпеки або ненадійних протоколів. Основна мета цього аналізу — знайти та усунути вразливості або помилки до того, як вони потраплять у продуктивне середовище.

Основна перевага перегляду коду полягає в тому, що він дозволяє виявляти та виправляти проблеми на ранніх етапах розробки, що в кінцевому результаті допомагає зекономити час і ресурси. Він також дозволяє виявляти та виправляти проблеми, які можуть бути пропущені під час тестування.

Однак цей процес має і свої недоліки. Перегляд коду може бути трудомістким, особливо для великих систем. Крім того, його ефективність залежить від знань та досвіду осіб, які проводять перевірку, тому деякі проблеми, особливо пов'язані з новітніми методами атак, можуть залишитися невиявленими.

-Оцінка ризику: це систематичний процес ідентифікації та аналізу потенційних загроз і вразливостей, які можуть вплинути на веб-ресурс. Основна мета — оцінка ймовірності та можливих наслідків цих загроз, що допомагає визначити пріоритети в питаннях безпеки та розробити стратегію їх вирішення.

Основна перевага оцінки ризику полягає в тому, що вона дозволяє передбачати та своєчасно реагувати на потенційні проблеми безпеки, що може допомогти уникнути втрати даних, перебоїв у роботі або інших негативних наслідків.

Однак цей метод також має свої недоліки. Він може бути трудомістким і складним, особливо для великих організацій з комплексними системами. Його ефективність значною мірою залежить від точності та повноти використаних даних. Наприклад, оцінка ризику може не враховувати нові або невідомі загрози, що може призвести до недооцінки ризику.

Важливо зазначити, що найкращий підхід до забезпечення захищеності веб-ресурсу включає комбінацію різних методів. Такий комплексний підхід забезпечує виявлення та вирішення всіх потенційних вразливостей.

2.7.3 Принцип оцінювання рейтингу властивостей

Після завершення процесу сканування за допомогою системи Acunetix створюються ретельні звіти, що містять повну інформацію про всі ідентифіковані вразливості. Такі звіти включають докладний опис кожної проблеми, рекомендації щодо її уникнення і усунення та оцінку ступеня її серйозності. На даному етапі проводитемиться аналіз отриманих результатів та створення рекомендацій щодо покращення захисту системи Atutor. Оцінка вразливостей, виявлених завдяки Acunetix, проводиться відповідно до стандарту CVSS3.

Система оцінки серйозності вразливостей (CVSS) є вагомим інструментом для оцінки комп'ютерних загроз. Цей стандарт був розроблений Форумом Безпеки Інформаційних Систем (FIRST) на початку 2000-х років з метою стандартизації процесу оцінки рівня серйозності вразливостей.CVSS пройшов кілька етапів вдосконалення з часу його впровадження. Останнє покоління, CVSSv3, було випущене у 2015 році і представляє сучасну версію стандарту. Ця версія враховує більше факторів і дозволяє більш точно оцінювати рівень серйозності вразливостей.

-CVSSv1. Перше покоління CVSS було випущено у 2005 році. Воно ввело ряд базових метрик для оцінювання вразливостей, включаючи вплив на конфіденційність, цілісність та доступність системи.

-CVSSv2. Випущене у 2007 році, друге покоління CVSS внесло кілька покращень і додало темпоральні та середовищні метрики, які дозволили оцінити вразливості в контексті конкретного середовища, враховуючи такі фактори, як наявність виправлень або знань про вразливості.

-CVSSv3. Третє покоління, запущене у 2015 році, принесло більше гнучкості та точності. Ця версія збільшила кількість метрик, уточнила оцінки та додала додаткові класифікації вразливостей. Зокрема, CVSSv3 враховує такі фактори, як спосіб атаки, вимога до взаємодії з користувачем та обсяг впливу вразливості. CVSS дає змогу компаніям, органам управління безпекою та дослідникам з усього світу використовувати єдину, стандартизовану шкалу для оцінки рівня серйозності вразливостей, враховуючи широкий спектр факторів, що можуть вплинути на загальний вплив вразливості.

CVSSv3 використовує векторний підхід для оцінки вразливостей, який включає кілька ключових метрик. Цей вектор вказує на значення кожної метрики в форматі "метрика:значення". Разом вони формують CVSSv3 вектор, який допомагає визначити кінцеву оцінку вразливості. Метрики вектора поділяються на три групи: базові, темпоральні та середовищні

Базові Метрики:

Ці метрики оцінюють характеристики вразливості, які не змінюються з часом:

- Attack Vector (AV): вимірює, як атака може бути здійснена. Може бути Network (N), Adjacent (A), Local (L), або Physical (P).

- Attack Complexity (AC): вимірює, скільки умов поза контролем зловмисника має бути виконано, щоб атака була успішною. Може бути Low (L) або High (H).
- Privileges Required (PR): вказує, чи потрібні привілеї для успішного використання вразливості. Може бути None (N), Low (L), або High (H).
- User Interaction (UI): чи потрібна взаємодія користувача для експлуатації вразливості. Може бути None (N) або Required (R).
- Scope (S): чи впливає вразливість на інші компоненти, крім того, який був компрометований. Може бути Unchanged (U) або Changed (C).
- Confidentiality, Integrity and Availability Impact (C, I, A): вимірюють вплив вразливості на конфіденційність, цілісність та доступність системи. Може бути None (N), Low (L) або High (H).

Після визначення всіх цих метрик, вони об'єднуються в CVSSv3 вектор, який виглядає приблизно так:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

В цьому випадку:

Attack Vector - мережевий (N)
Attack Complexity - низька (L)
Privileges Required - відсутні (N)
User Interaction - відсутня (N)
Scope - незмінено (U)
Confidentiality, Integrity and Availability Impact - високий (H)

Ця методика дозволяє формувати реалістичний і виважений погляд на ризики, з якими стикається організація, забезпечуючи стандартизований підхід до оцінки серйозності вразливостей. Кожна метрика вектора має певний бал залежно від її значення, а потім бали обраховуються разом для визначення загальної оцінки вразливості.

Діапазон оцінок від 0 до 10 застосовується задля визначення серйозності вразливостей згідно з CVSSv3. Чим вищий рейтинг, тим серйозніша вразливість. Загалом, оцінки можуть мати такий характер

- 0.0 - вразливість відсутня або незначна.

- 0.1 - 3.9 - низький рівень серйозності. Вразливість може бути легко використана або мати обмежений вплив.
- 4.0 - 6.9 - середній рівень серйозності. Вразливість може бути помірно складною для використання або мати помірний вплив.
- 7.0 - 8.9 - високий рівень серйозності. Вразливість може бути складною для використання або мати значний вплив.
- 9.0 - 10.0 - дуже високий рівень серйозності. Вразливість може бути легко використана або мати критичний вплив.

Такий діапазон допомагає визначити серйозність вразливостей та встановити пріоритети для їх виправлення у системах. Ці оцінки використовуються в базі даних National Vulnerability Database (NVD), яка надає дані щодо вразливості, а також їх серйозність для безпечної спільноти. На основі вказаних метрик проводиться оцінка кожної вразливості. Проте, важливо зазначити, що дані метрики не враховують місця виявлення вразливості та можливу чутливу інформацію, яка може знаходитися у зоні впливу цієї вразливості. Тому під час оцінки вразливостей, виявлених у Atutor, використовується оцінка, надана сканером Acunetix, а також враховується потенційний вплив цих вразливостей на критичні активи системи.

3 Спеціальна частина

3.1 Алгоритм взаємодії студента з камерою. Блок-схема

Взаємодія з камерою студента здійснюється через API "Media Capture and Streams", підтримуваний більшістю сучасних браузерів. Перед початком тестування зображення з камери проходять перевірку автентичності за допомогою цього API, який видає токен для доступу до тесту.

Під час тесту зображення регулярно надсилаються на сервер і зберігаються у форматі jpeg. Після завершення тестування сервіс обробки стискає зображення за допомогою кодека VP9, зберігаючи їхню якість, і пакує їх у контейнер "WebM". Це дозволяє зменшити обсяг даних на диску в 7-9 разів. Потім зображення вилучаються з контейнера для подальшої обробки.

На наступному етапі здійснюється розпізнавання та порівняння з фото особи в університетській базі даних. Сервіс розпізнавання базується на бібліотеках dlib, face_recognition і cv2, а API реалізовано за допомогою мікрофреймворку "Flask". Розпізнавання починається з пошуку обличчя на зображенні, використовуючи комбінацію двох моделей з dlib: спочатку застосовується ефективніша та швидша модель на основі гістограм орієнтованих градієнтів (HOG) і лінійного SVM-класифікатора, а якщо вона не спрацьовує, використовується точніша, але повільніша модель на основі згорткової нейронної мережі (CNN). Після цього обличчя розпізнається за допомогою моделі dlib_face_recognition_resnet_model_v1, яка є залишковою нейронною мережею (ResNet) з 29 шарами.

Ця модель була навчена на наборі з трьох мільйонів облич і забезпечує точність 99,38% у тесті "Labeled Faces in the Wild". В результаті роботи моделі формується 128-вимірний вектор, що описує обличчя. Отримані вектори для обличчя студента на зображеннях та обличчя на фото з університетської бази даних порівнюються за евклідовою відстанню, на основі якої робиться висновок про їхню схожість. Сервіс обробки додає висновок про схожість облич до результатів тесту в LMS ATutor разом із повним записом зображень, доступних для перегляду. Впровадження таких технічних рішень у систему електронного навчання дозволяє значно обмежити та контролювати недобросовісне проходження тестів у дистанційному навчанні.

Блок-схема

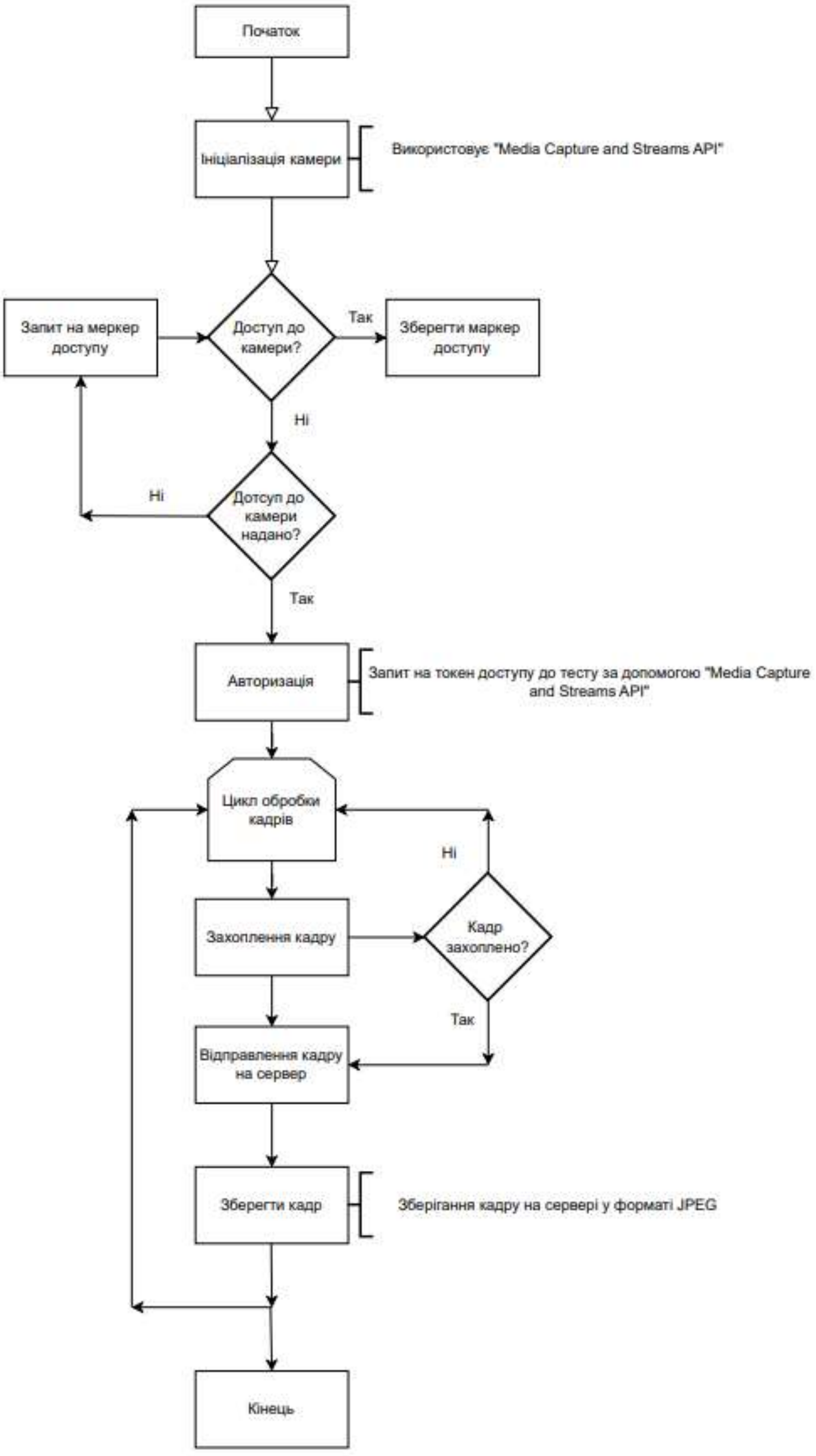


Рисунок 3.1 Блок-схема алгоритму взаємодії

3.2 SQL-запити для відображення деяких даних системи LMS Atutor

Таблиця 3.1 –Кількість студентів, які використовують систему навчання в період 2021- 2024рр.

Роки	Кількість юзерів-студентів
2021/22	3841

2022/23	4636
2023/24	6304

Рисунок 3.2 Відображення даних таблиці 3.1 у вигляді діаграми

Рисунок 3.3 Відображення даних таблиці 3.1 у вигляді графіку

Таблиця 3.2 – Кількість викладачів, які використовують систему навчання в період 2021-2024рр.

Роки	Кількість юзерів-викладачів
2021/22	405

2022/23	410
2023/24	403

Рисунок 3.4 – Відображення даних таблиці 3.2 у вигляді діаграми

Рисунок 3.5 – Відображення даних таблиці 3.2 у вигляді графіку

Таблиця 3.3 – Кількість тестів, зданих в системі навчання в період 2021-2024рр.

Місяць	**Тестів здано**	**Тестів здано із веб-**

		камерою
2021-09	3921	0
2021-10	20729	1457
2021-11	46383	2777
2021-12	44527	3998
2022-01	3000	590
2022-02	2640	134
2022-03	4334	126
2022-04	19036	1275
2022-05	33249	2473
2022-06	42199	3127
2022-07	1164	148
2022-08	200	11
2022-09	1961	44
2022-10	10920	543
2022-11	33246	4370
2022-12	68319	10443
2023-01	13897	1573
2023-02	4293	385
2023-03	7546	612
2023-04	19877	2810
2023-05	35086	4304
2023-06	58846	7794
2023-07	3470	412
2023-08	613	63
2023-09	4164	169
2023-10	21692	4863
2023-11	48370	9276
2023-12	70788	14104
2024-01	3695	669
2024-02	3778	447
2024-03	9957	1708
2024-04	22834	4997

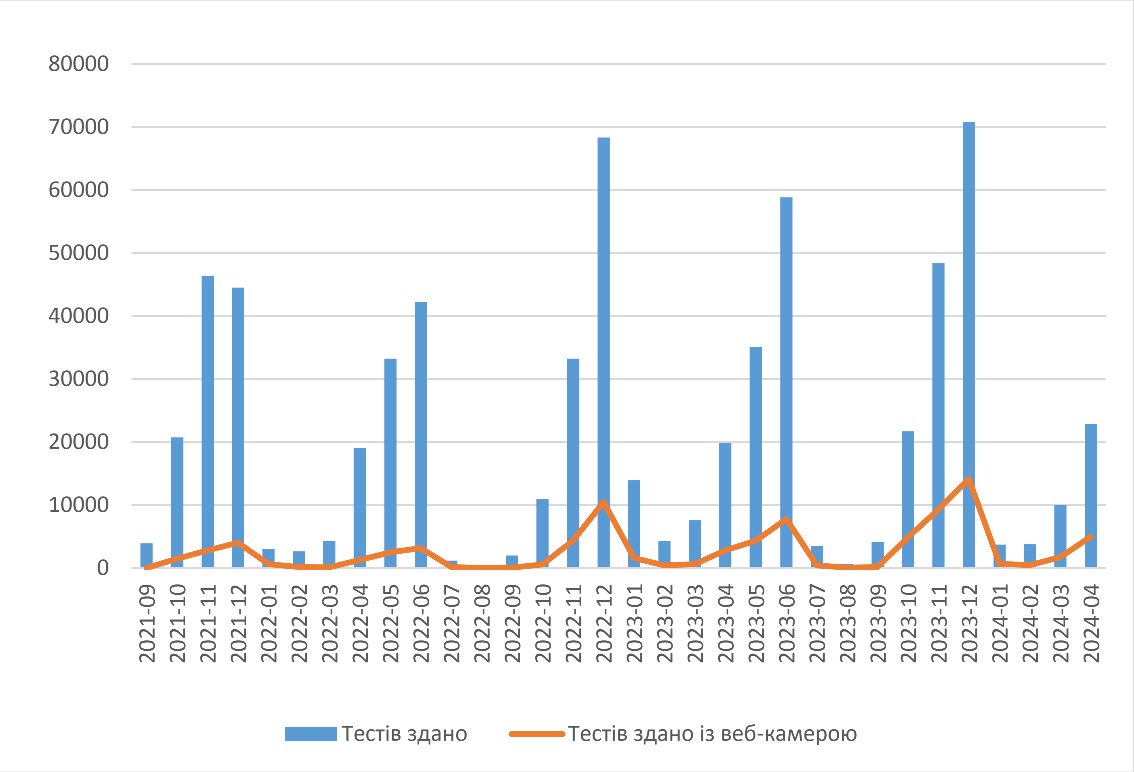


Рисунок 3.6 – Відображення даних таблиці 3.3 у вигляді графіку

Таблиця 3.4 – Типи пристроїв, з яких виконується вхід в систему навчання в період 2021-2024рр. та їх відсоткове значення

Роки	тип пристрою	кількість юзерів
2021/22	mobile	60%
2021/22	dekstop	39,30%
2021/22	tablet	0,65%
Роки	тип пристрою	кількість юзерів
2022/23	mobile	64,34%
2022/23	dekstop	34,92%
2022/23	tablet	0,74%
Роки	тип пристрою	кількість юзерів
2023/24	mobile	59,15%
2023/24	dekstop	40,25%
2023/24	tablet	0,60%

Рисунок 3.7 – Відображення даних таблиці 3.4 у вигляді діаграми

Рисунок 3.8 – Відображення даних таблиці 3.4 у вигляді діаграми

Рисунок 3.9 – Відображення даних таблиці 3.4 у вигляді діаграми

Таблиця 3.5 – Кількість перевірених робіт на унікальність в період 01.2024-04.2024р.

місяці	кількість робіт перевірених на унікальність
2024-01	565
2024-02	1738
2024-03	4947
2024-04	5756

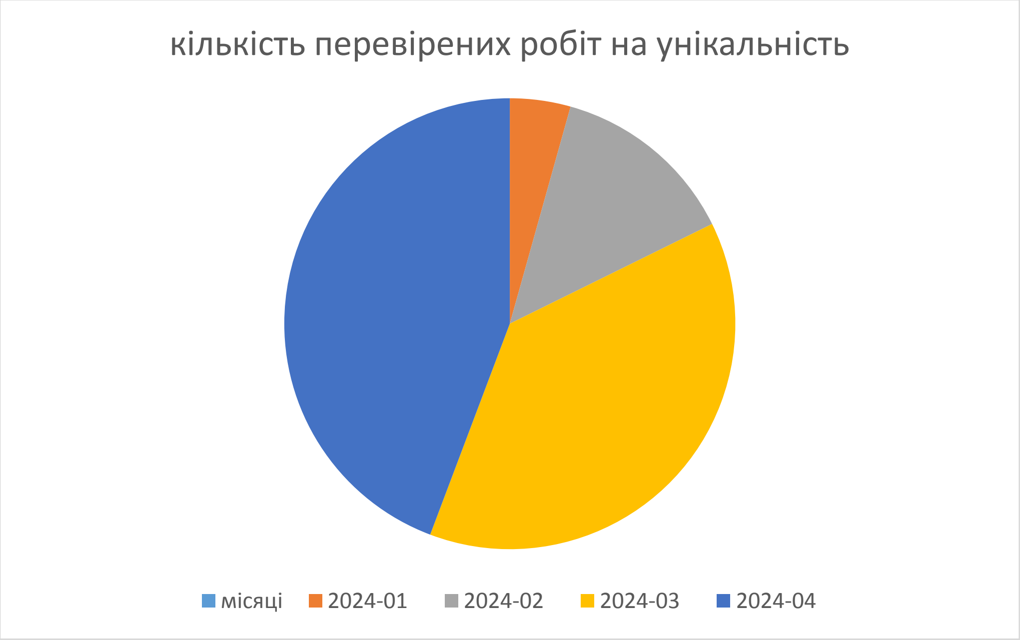


Рисунок 3.10 – Відображення даних таблиці 3.5 у вигляді діаграми

Рисунок 3.11 Відображення даних таблиці 3.5 у вигляді графіку

4 Безпека життєдіяльності та основи охорони праці

4.1 Ергономічні проблеми безпеки життєдіяльності при роботі за комп'ютером

У сучасному світі все більше людей проводять значну частину свого робочого часу за комп'ютером, що призводить до ряду ергономічних проблем, які негативно впливають на безпеку та здоров'я людей. Неправильна позиція тіла, незручне розташування робочого місця, тривале сидіння та напружена робота з клавіатурою та мишею спричиняють м'язове напруження, біль у спині та напругу очей, що викликає дискомфорт та незручності.

Розташування робочого місця відіграє важливу роль у забезпеченні безпеки та здоров'я під час роботи за комп'ютером. Оптимальна висота столу та стільця є ключовим фактором для забезпечення комфорту і підтримки правильної позиції тіла. Стіл належної висоту, щоб лікті могли спокійно розташовуватися на клавіатурі, а стопи - на підлозі. Стілець обладнаний підтримкою для спини та належними регульованими підлокітниками. Клавіатура розташована на рівні ліктів, монітор - належним чином вирівняний перед очима, а миша - в зоні доступу для зап'ястя.

Правильне розташування робочого місця сприяє уникненню незручностей та проблем зі здоров'ям. Ергономічні пристрої підтримки є корисними для забезпечення комфорту та запобігання напрузі м'язів. Використання регульованих підлокітників та підставок для зап'ястя допомагає знизити напругу на м'язах і запобігти незручностям. Оптимальне розташування робочого місця повинне враховувати індивідуальні особливості користувача та забезпечувати комфортні умови для роботи.

Правильна позиція тіла та рухи є ключовими факторами для забезпечення комфорту та запобігання напрузі м'язів та незручностям.

Важливо пам'ятати про правильну позицію спини та уникати підгорблення або надмірного нахилу голови під час тривалої роботи за комп'ютером. Регулярні перерви для розтяжки та руху є важливими для підтримання здоров'я. Прості фізичні вправи, такі як розтягування шиї, плечей, рук і ніг, допомагають зняти напругу з м'язів та покращити кровообіг. Регулярні перерви дозволяють розслабитися і зберегти енергію для продуктивної роботи. Очі є одними з найбільш вразливих органів під час роботи за комп'ютером. Постійне спрямування погляду на екран призводить до напруження та втому очей.

Для зменшення негативного впливу необхідно використовувати екрани з антибликовим покриттям, яке знижує відблиск та рефлексію світла. Також важливо налаштовувати яскравість та контрастність екрану для комфортного сприйняття. Щоб зменшити напругу на очі, необхідно робити перерви для відпочинку, фокусуючись на далеких предметах або виконуючи вправи для розслаблення очей.

Використання неправильної клавіатури та миші призводить до м'язового напруження і тунельного синдрому. Важливо використовувати ергономічні клавіатури та миші з додатковою підтримкою для зап'ястя та комфортною формою. Правильна позиція рук та зап'ястя під час роботи з ними має велике значення. Регулярні перерви для розтяжки рук та масажу зап'ястя допомагають уникнути негативних наслідків від тривалого використання клавіатури та миші. Розглядаючи ергономічні проблеми безпеки життєдіяльності при роботі за комп'ютером, варто зазначити, що їх вирішення є ключовим для забезпечення безпеки та здоров'я під час роботи.

Дотримання принципів ергономіки, налагодження робочого місця, правильна позиція тіла та виконання фізичних вправ сприяють покращенню безпеки та створенню здорового робочого середовища. Застосування ергономічних пристроїв підтримки, таких як регульовані підлокітники та підставки для зап'ястя, також сприяє комфорту та попередженню незручностей. Загальною метою є створення безпечного та здорового робочого середовища для людей, які працюють за комп'ютером та виконують дослідження захищеності веб сервісу електронного навчання Atutor, що забезпечує збереження здоров'я та підвищення продуктивності працівників, сприяє запобіганню травмам та ергономічним проблемам, а також сприяє загальному комфорту та задоволенню від роботи.

Додатково, важливо зазначити, що належна освітленість приміщення також є важливим фактором, який впливає на комфорт та здоров'я під час роботи за комп'ютером. Потрібно забезпечити достатнє природне або штучне освітлення, яке не перевантажує очі. Розміщення робочого місця біля вікна або використання належної освітлювальної техніки допомагає забезпечити оптимальні умови освітлення.

Важливо також уникати відблисків на екрані, розташовуючи монітор під правильним кутом до джерел світла. Безпека та конфіденційність інформації також є важливим аспектом при роботі за комп'ютером. Важливо зберігати конфіденційні дані та захищати їх від несанкціонованого доступу. Використання паролів, шифрування даних та регулярне оновлення програмного забезпечення допомагає забезпечити безпеку інформації.

Крім того, необхідно усвідомлювати потенційні загрози з боку шкідливих програм та фішингових атак і приймати заходи для їх запобігання, такі як використання антивірусного програмного забезпечення та обережне відкривання електронних листів та посилань. Регулярне навчання та свідомість про важливість ергономіки та безпеки при роботі за комп'ютером є важливими.

Працівники повинні мати бути проінформовані про правильні методи роботи, виконання пауз і фізичних вправ, а також процедур безпеки. Організації можуть проводити навчання та інформаційні тренінги, щоб підвищити свідомість та забезпечити правильну поведінку під час роботи за комп'ютером.

Враховуючи всі ці аспекти, створення комфортного, безпечного та здорового робочого середовища є важливим завданням як для працівників, так і для роботодавців. Захист здоров'я та добробуту працівників при роботі за комп'ютером не тільки покращує їхню якість життя, але й сприяє збільшенню продуктивності та задоволення від роботи, що має позитивний вплив на всю організацію.

4.2 Організація безпечної роботи електроустаткування задіяного при роботі системи електронного навчання

Безпечна робота електроустаткування є ключовим елементом для забезпечення стабільної та безперебійної роботи системи електронного навчання. Це включає в себе правильне проектування, встановлення, експлуатацію та обслуговування електроустаткування. Дотримання стандартів і правил охорони праці допомагає мінімізувати ризики електричних ударів, пожеж та інших небезпек.

Перед встановленням електроустаткування необхідно ретельно оцінити його відповідність вимогам системи електронного навчання. Вибір обладнання повинен базуватися на таких критеріях:

надійність та безпека: обладнання має відповідати стандартам якості та безпеки, мати сертифікати відповідності та бути розрахованим на довготривалу експлуатацію; відповідність технічним вимогам: обладнання повинно підтримувати необхідні технічні параметри, такі як напруга, потужність, тип з'єднання тощо;сумісність з іншими компонентами: всі компоненти системи повинні бути сумісні між собою, щоб уникнути збоїв та небезпек при експлуатації;

Під час встановлення необхідно дотримуватися таких заходів безпеки:

правильне заземлення: всі пристрої повинні бути заземлені відповідно до норм, щоб уникнути накопичення статичної електрики та можливості

удару струмом;використання захисних пристроїв: встановлення автоматичних вимикачів, пристроїв захисного вимкнення (ПЗВ) та інших захисних засобів є обов’язковим для забезпечення безпеки;
професійний монтаж: монтаж повинен виконуватися кваліфікованими спеціалістами з дотриманням всіх норм і правил;

Для забезпечення безпечної експлуатації електроустаткування слід дотримуватися таких рекомендацій:регулярний контроль та технічне обслуговування: обладнання повинно регулярно перевірятися на наявність зношення, перегріву, пошкоджень проводів та інших дефектів. Технічне обслуговування повинно проводитися відповідно до інструкцій виробника; контроль температурного режиму: устаткування не повинно перегріватися. Необхідно забезпечити достатню вентиляцію та уникати розташування пристроїв поблизу джерел тепла; правильне використання: обладнання має використовуватися тільки за призначенням, з дотриманням інструкцій та рекомендацій виробника;

При обслуговуванні та ремонті електроустаткування необхідно дотримуватися таких заходів безпеки: відключення живлення: перед проведенням будь-яких робіт обладнання має бути відключене від джерела живлення; використання засобів індивідуального захисту (ЗІЗ): спеціалісти повинні використовувати відповідні ЗІЗ, такі як діелектричні рукавички, килимки, інструменти з ізоляційними покриттями;
дотримання процедур: всі ремонтні роботи повинні проводитися відповідно до технічних інструкцій та нормативних документів;

Управління ризиками та навчання персоналу є невід'ємною частиною забезпечення безпеки електроустаткування: ідентифікація ризиків: постійний аналіз можливих ризиків та їх мінімізація є ключовим аспектом безпеки. Для цього проводяться регулярні оцінки стану обладнання та аналіз умов експлуатації; навчання та інструктажі: персонал повинен проходити регулярні навчання та інструктажі з питань безпечної роботи з електроустаткуванням. Це включає як базові знання, так і спеціальні навички для роботи з конкретними видами обладнання;

розробка та впровадження процедур безпеки: необхідно розробити детальні інструкції та процедури з безпеки, які повинні бути доступними для всіх працівників та регулярно оновлюватися.

Таким чином, організація безпечної роботи електроустаткування задіяного при роботі системи електронного навчання вимагає комплексного підходу, що включає вибір надійного обладнання, правильне його встановлення, регулярне технічне обслуговування, навчання персоналу та управління ризиками. Дотримання цих заходів дозволяє забезпечити стабільну та безпечну роботу системи, що є критично важливим для ефективного функціонування освітнього процесу.

Висновок

У цій роботі досліджено й проаналізовано наявні методи верифікації особи під час контролю знань в освітніх установах, а також розроблено автоматизовану систему, яка інтегрується в систему управління навчанням (LMS) ATutor.

На основі проведеного аналізу обрано ефективну комбінацію алгоритмів для виявлення та розпізнавання облич: гістограми напрямлених градієнтів (HOG) у поєднанні з методом опорних векторів (SVM) та глибинними згортковими нейронними мережами (CNN).

Основні висновки роботи:

1. Аналіз існуючих рішень: комерційні рішення, що є на ринку, не дозволяють повноцінно інтегруватися з популярними системами електронного навчання і не забезпечують високої точності розпізнавання, що вимагає подальших досліджень та розробок.
2. Вибір алгоритмів: обрані алгоритми HOG та SVM забезпечують високу швидкість і точність виявлення облич, тоді як глибинні нейронні мережі (ResNet) з 29 шарами, натреновані на великому наборі даних, досягають точності 99.38% у тестах.
3. Розробка та інтеграція системи: система фотофіксації та верифікації особи була успішно інтегрована в LMS ATutor. Ця система використовує веб-технології та високоефективні засоби розпізнавання особи, що мінімізує витрати на впровадження і дозволяє використовувати наявне програмно-апаратне забезпечення користувачів.
4. Ефективність системи: проведені дослідження підтвердили, що розроблена система ефективно працює в реальних умовах контролю знань, забезпечуючи автоматичну та точну верифікацію особи.

Таким чином, розроблена система верифікації особи для контролю знань в освітніх установах демонструє високу ефективність та потенціал для широкого впровадження в існуючі системи електронного навчання.

Список використаної літератури

1. Дячук С. Ф., Коноваленко І. В., Шкодзінський О. К. Віртуальне навчальне середовище Тернопільського національного технічного університету імені Івана Пулюя на базі LMS ATutor. *Теорія і практика дистанційного навчання іноземних громадян: вітчизняний та міжнародний досвід* : Міжнар. наук.-практ. семінар, м. Харків, 12 листоп. 2014 р. Харків: ХНУРЕ, 2014. С. 11–15. URL: https://core.ac.uk/download/pdf/60800333.pdf (дата звернення: 25.05.2023).
2. Сас Д. Аналіз результатів роботи модуля фотофіксації та розпізнавання особи у системі електронного навчання ТНТУ *Природничі та гуманітарні науки. Актуальні питання*, VI Міжнародна студентська науково - технічна конференція, м. Тернопіль, 27-28 квітня 2023 р. (збірник тез конференції). Тернопіль: ТНТУ, 2023. С. 21–22. URL: https://elartu.tntu.edu.ua/bitstream/lib/41140/1/ Zbirnyk_2023.pdf#page=21 (дата звернення: 25.05.2023).
3. Шкодзінський О., Луцків М., Смолій М. Розвиток засобів верифікації особи та її дій при контролі знань в умовах дистанційного навчання. *Актуальні задачі сучасних технологій* : Зб. тез доп. X Міжнар. науково-практ. конф. молодих уч. та студентів, м. Тернопіль, 24 листоп. 2021 р. Тернопіль: ТНТУ, 2021. С. 138–139. URL: https://elartu.tntu.edu.ua/handle/lib/36486 (дата звернення: 25.05.2023).
4. Платформа .NET та мова програмування C# 8.0: навчальний посібник / Коноваленко І.В., Марущак П.О. – Тернопіль: ФОП Паляниця В. А., 2020 – 320 с. /Рекомендовано до друку Вченою радою Тернопільського національного технічного університету імені Івана Пулюя. Протокол № 10 від 20 жовтня 2020 року
5. Савків В.Б., Капаціла Ю.Б., Михайлишин Р.І. Методичні вказівки до виконання кваліфікаційної роботи бакалавра спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології». Тернопіль.: Видавництво ТНТУ. 2021. 50 с. https://elartu.tntu.edu.ua/handle/lib/35172

6. Автоматизація виробничих процесів. Навчальний посібник для технічних спеціальностей вищих навчальних закладів. / Я.І. Проць, В.Б. Савків, О.К. Шкодзінський, О.Л. Ляшук. Тернопіль: ТНТУ ім. І. Пулюя, 2011. 344 с.
7. Автоматизація періодичних технологічних процесів: Типова програма, методичні вказівки, теорія та практика. Лабораторний практикум / Укладачі: Проць Я.І., Данилюк О.А.. Федорів П.С. - Тернопіль: ТДТУ, 2005 -135 с.
8. Методичні вказівки для написання розділу «Безпека життєдіяльності, основи охорони праці» в кваліфікаційних роботах здобувачів освітнього рівня „бакалавр”. Для студентів всіх форм навчання рівень вищої освіти перший (бакалаврський)/ укл.: О. Я. Гурик , І. Б. Окіпний. – Тернопіль: ТНТУ імені Івана Пулюя, 2021. - 20 с.
9. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі. Книга 1 [навчальний посібник]. Львів : «Магнолія 2006», 2013. 256 с.
10. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі. Книга 2. [навчальний посібник]. Львів : "Магнолія 2006", 2014. 312 с.
11. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі : навчальний посібник. Книга 1. Львів : «Магнолія 2006». 2013. 256 с.
12. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.
13. ATutor Features [Електронний ресурс]. – Режим доступу: https://atutor.github.io/atutor/features.html
14. ATutor Learning Management System [Електронний ресурс]. – Режим доступу: https://atutor.github.io/atutor/index.html
15. Atutor Atutor : CVE security vulnerabilities, versions and detailed reports [Електронний ресурс]. – Режим доступу: https://www.cvedetails.com/product/13342/Atutor-Atutor.html?vendor_id=7805

16. Main features of ATutor [Електронний ресурс]. – Режим доступу: https://dl.tntu.edu.ua/downloads/Main-features.pdf
17. ATutor Developer Guidelines [Електронний ресурс]. – Режим доступу: https://atutor.github.io/developer/guidelines.html
18. ATutor at Ternopil Ivan Puluj National Technical University [Електронний ресурс]. – Режим доступу: https://dl.tntu.edu.ua/showpage.php?id=8
19. AContent Learning Content Management System (LCMS) [Електронний ресурс]. – Режим доступу: https://atutor.github.io/acontent/index.html
20. What are the different information classification categories available in TCS? [Електронний ресурс] // Helpr.me. – Режим доступу: https://uk.helpr.me/2722-what are-the-different-information-classification-categories-available-in-tcs
21. Technical evaluation of information environment security | EY Ukraine [Електронний ресурс] // EY Ukraine. – Режим доступу: https://www.ey.com/uk_ua/consulting/technical-evaluation-of-informationenvironment-security
22. CVSS V3 Calculator | NIST National Vulnerability Database (NVD) [Електронний ресурс] // NIST National Vulnerability Database (NVD). – Режим доступу: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
23. CVSS v3 User Guide | FIRST.org, Inc. [Електронний ресурс] // FIRST.org, Inc. – Режим доступу: https://www.first.org/cvss/v3.0/user-guide
24. CVSS v3 Metrics | NIST National Vulnerability Database (NVD) [Електронний ресурс] // NIST National Vulnerability Database (NVD). – Режим доступу: https://nvd.nist.gov/vuln-metrics/cvss
25. Static and Dynamic Testing Methods | QATestLab Blog [Електронний ресурс] // QATestLab Blog. – Режим доступу: https://training.qatestlab.com/blog/technical-articles/static-and-dynamic-testingmethods/
26. Huber, B., & Gambardella, L., Occupational Ergonomics: Principles and Applications. 18. Smith, J., Brown, A., & Johnson, C., Management of fractures: an overview // Journal of Orthopedic Trauma. – 2018. – DOI