ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті»
коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Программалық инженерия кафедрасы

Тілеуқабақов Руслан Алғабайұлы

«Тауарларды өндірушілер мен импорттаушылардың несиелік қабілетін бағалауға арналған машиналық оқыту үлгілері»

6B06102 – Computer science

ДИПЛОМДЫҚ ЖҰМЫС

Алматы 2025

АҢДАТПА

Бұл дипломдық жұмыс тауарларды өндірушілер мен импорттаушылардың несиелік қабілетін бағалау үшін машиналық оқыту (machine learning) үлгілерін әзірлеуге және зерттеуге арналған. Жұмыстың өзектілігі қаржы ұйымдарының несие беру кезінде тәуекелдерді төмендетуге ұмтылуымен, сондай-ақ дәстүрлі бағалау әдістерінің шектеулілігімен және үлкен деректерді талдауға негізделген заманауи шешімдерге деген сұраныстың артуымен байланысты.

Жұмыстың мақсаты – машиналық оқыту алгоритмдерін пайдалана отырып, өндіруші және импорттаушы компаниялардың қаржылық тұрақтылығы мен несиелік қабілетін дәл болжай алатын модель құру. Жобада логистикалық регрессия, шешім ағаштары, кездейсоқ ормандар (Random Forest), және градиентті бустинг (XGBoost) секілді алгоритмдер салыстырылып, олардың тиімділігі мен дәлдігі талданады.

Бағалау жүйесі Python тілінде жасалған, деректер PostgreSQL мәліметтер қорында сақталады, ал пайдаланушымен өзара әрекеттесу React арқылы құрылған веб-интерфейс арқылы жүзеге асырылады. Жүйенің деректер көзі ретінде компаниялардың қаржылық есептері, салық төлеу тарихы, импорт көлемі, келісімшарттар және төлем тәртібі сияқты параметрлер қарастырылады. Модельдердің сапасы кросс-валидация және негізгі метрикалар (дәлдік, нақтылық, еске түсіру, F1 көрсеткіші) арқылы бағаланады. Бұл жұмыс қаржы ұйымдарына несиелік шешімдерді автоматтандыруға, тәуекелдерді азайтуға және сапалы клиенттерді таңдауға мүмкіндік беретін құрал әзірлеуге бағытталған.

АННОТАЦИЯ

Данная дипломная работа посвящена разработке и исследованию моделей машинного обучения для оценки кредитоспособности производителей и импортеров. Актуальность темы обусловлена стремлением финансовых организаций снизить риски при выдаче кредитов, ограниченностью традиционных методов оценки и растущей потребностью в современных решениях, основанных на анализе больших данных.

Цель работы — построить модель, способную точно прогнозировать финансовую устойчивость и кредитоспособность компаний-производителей и импортеров с использованием алгоритмов машинного обучения. В проекте рассматриваются и сравниваются такие алгоритмы, как логистическая регрессия, деревья решений, случайный лес (Random Forest) и градиентный бустинг (XGBoost), проводится их оценка по эффективности и точности. Система оценки разработана на языке Python, данные хранятся в базе данных PostgreSQL, а пользовательский интерфейс реализован с использованием React.

В качестве входных данных используются финансовые отчеты компаний, история налоговых платежей, объем импорта, выполнение контрактов и платежная дисциплина. Эффективность моделей оценивается с помощью кросс-валидации и ключевых метрик (точность, полнота, F1-мера). Работа направлена на создание инструмента, который поможет автоматизировать процесс принятия кредитных решений, снизить риски и выявить надежных клиентов.

ANNOTATION

This diploma work is dedicated to the development and research of machine learning models for assessing the creditworthiness of manufacturers and importers. The relevance of the study stems from the need of financial institutions to minimize risks in lending decisions, the limitations of traditional assessment methods, and the growing demand for modern solutions based on big data analysis.

The main goal of the work is to build a model that can accurately predict the financial stability and credit capacity of manufacturing and importing companies using machine learning algorithms. The project compares algorithms such as logistic regression, decision trees, random forest, and gradient boosting (XGBoost), evaluating their effectiveness and accuracy.

The assessment system is developed using Python, with data stored in a PostgreSQL database, and the user interface is implemented with React. The model uses input data such as financial reports, tax payment history, import volume, contract performance, and payment discipline. Model performance is evaluated through cross-validation and key metrics such as accuracy, precision, recall, and F1-score. This project aims to provide a tool for financial institutions to automate credit decision-making, reduce risks, and identify reliable clients.

МАЗМҰНЫ

	КІРІСПЕ	6
1	Онлайн банк жүйелеріндегі аутентификация және авторизация әдістерінің аналитикалық шолуы	7
1.1	Нарықты талдау	7
1.1.1	Нарықтағы негізгі монополисттер	7
1.1.2	Банктік киберқауіпсіздік нарығына шолу	8
1.1.3	Аймақтық салыстыру	9
1.1.4	Болашақтағы тенденциялар мен нарықтың болашағы	10
1.2	Барлық аналогтардың салыстырмалы талдауы	11
1.2.1	Қауіпсіздік деңгейі	12
1.2.2	Қолданылуы	13
1.2.3	Интеграция	14
1.2.4	Қауіптерге бейімделу қабілеті	15
1.2.5	Банктік инфрақұрылыммен интеграция	15
1.2.6	Банктік инфрақұрылы қорытынды	16
1.3	Жобаның сипаттамасы	17
1.3.1	Жобаның мақсаттары	17
1.3.2	Сұраныстармен жұмыс істеу принципі тіркеу мысалы негізінде қарастырылады	18
1.3.3	Жобаның негізгі құрамдас бөліктері	19
2	Теориялық бөлім	24
2.1	Жобаның жалпы архитектурасы	24
2.2	Қорғау жүйесінің құрылымдық сипаттамасы	27
2.3	ERD диаграмма	31
2.4	AI моделінің құрылымдық сипаттамасы	32
3	Практикалық бөлім	35
3.1	Қолданылған технологиялар мен құралдар	35
3.2	Аутентификация мен авторизацияны жүзеге асыру	35
3.2.1	Пайдаланушының аутентификация процесі	36
3.2.2	Пайдаланушының авторизациясы	36
3.2.3	Сеансты басқару және қауіпсіздікті жақсартулар	37
3.3	Деректер базасын енгізу және оңтайландыру	37
3.3.1	Мәліметтер қорының құрылымы	37
3.3.2	Қауіпсіздік шаралары	38
3.4	Модельді әзірлеу, машиналық оқыту.	38
	ҚОРЫТЫНДЫ	46
	ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ	48

КІРІСПЕ

Дипломдық жобаның тақырыбы – «Тауарларды өндірушілер мен импорттаушылардың несиелік қабілетін бағалауға арналған машиналық оқыту үлгілері». Бұл жобаның өзектілігі қазіргі заманғы қаржы институттарының несие беру шешімдерінде тәуекелдерді азайту қажеттілігіне, дәстүрлі бағалау әдістерінің шектеулігіне және үлкен деректерді (Big Data) сараптауға негізделген заманауи шешімдерге деген сұраныстың артуына байланысты туындайды.

Өндірушілер мен импорттаушылардың қаржылық тұрақтылығын дәлірек болжауға мүмкіндік беретін интеллектуалды жүйелер әзірлеу — қазіргі заманғы экономиканың талаптарына толық сай келетін маңызды бағыттардың бірі. Жобаның басты мақсаты – машиналық оқыту алгоритмдерін пайдалана отырып, компаниялардың несие қабілетін тиімді бағалайтын үлгіні әзірлеу. Бұл мақсатқа жету үшін логистикалық регрессия, шешім ағаштары, Random Forest және XGBoost секілді алгоритмдер салыстырылып, олардың дәлдігі мен тиімділігі зерттеледі. Бағалау жүйесі Python бағдарламалау тілінде әзірленіп, деректер PostgreSQL мәліметтер қорында сақталады. Жүйенің веб-интерфейсі React кітапханасының көмегімен жүзеге асырылады.

Үлгілерге енгізілетін негізгі деректер ретінде компанияның қаржылық есептері, салық төлемдерінің тарихы, импорт көлемі, шарттарды орындау деңгейі және төлем тәртібі қарастырылады. Үлгілердің сапасы кросс-валидация әдісі және дәлдік (accuracy), нақтылық (precision), толықтық (recall), F1 көрсеткіші арқылы бағаланады. Жобаның практикалық маңыздылығы — қаржы ұйымдарына сенімді және автоматтандырылған шешім қабылдау жүйесін ұсыну. Бұл жүйе несиелеу барысында тәуекелдерді төмендетіп, сенімді клиенттерді анықтауға көмектеседі. Зерттеу барысында бақылау, модельдеу, эксперимент жүргізу, логикалық тұжырымдау, стандарттарды сараптау және тестілеу әдістері қолданылды.

Дипломдық жұмыс кіріспеден, аналитикалық және теориялық бөлімдерден, практикалық жүзеге асырудан, экономикалық тиімділік негіздемесінен және қорытындыдан тұрады.

1 Онлайн банк жүйелеріндегі аутентификация және авторизация әдістерінің аналитикалық шолуы

1.1 Нарықты талдау

Онлайн банкинг жүйелеріндегі аутентификация және авторизация әдістері цифрлық транзакциялардың қауіпсіздігін қамтамасыз етудің маңызды бөлігіне айналды. Себебі киберқауіптер жыл өткен сайын күрделеніп келеді. Қаржы операцияларын жүргізу үшін қолданушылардың көпшілігі цифрлық арналарды таңдаған сайын, банктер киберқылмыстардың — оның ішінде жеке деректерді ұрлау, фишинг, рұқсатсыз қол жеткізу сияқты қауіптердің алдын алу үшін сенімді қауіпсіздік механизмдерін енгізуге мәжбүр.

Дәстүрлі құпиясөзге негізделген жүйелер фишинг, логин/парольді ұрлау және брутфорс шабуылдары сияқты қауіптерге жиі тап болуда. Бұл өз кезегінде клиенттердің қаржылық деректерінің қауіпсіздігіне нұқсан келтіруі мүмкін. Осыған байланысты қаржы ұйымдары қосымша қауіпсіздік деңгейлерін қамтамасыз ету мақсатында көпфакторлы аутентификация (MFA), биометрикалық жүйелер сияқты заманауи әдістерді енгізіп жатыр. Мұндай шешімдер қолданушы деректерінің қауіпсіздігін арттырып қана қоймай, банктің беделін де сақтап қалуға көмектеседі. Бұл бөлімде онлайн банк жүйелерінде қолданылатын заманауи қауіпсіздік әдістері мен осы саладағы нарықтың қазіргі жағдайына талдау жасалады.

1.1.1 Нарықтағы негізгі монополисттер

Несиелік қабілетті бағалау нарығы қаржы институттары үшін маңызды болып табылады, себебі ол рискті басқаруға, несиелік шешімдерді жақсартуға және реттеуші талаптарды орындауға көмектеседі. Жасанды интеллект технологияларының дамуымен машиналық оқыту негізіндегі несиелік қабілетті бағалау шешімдері кеңінен таралуда. Бұл саладағы негізгі ойыншылар мен технологиялық платформаларға мыналар жатады:

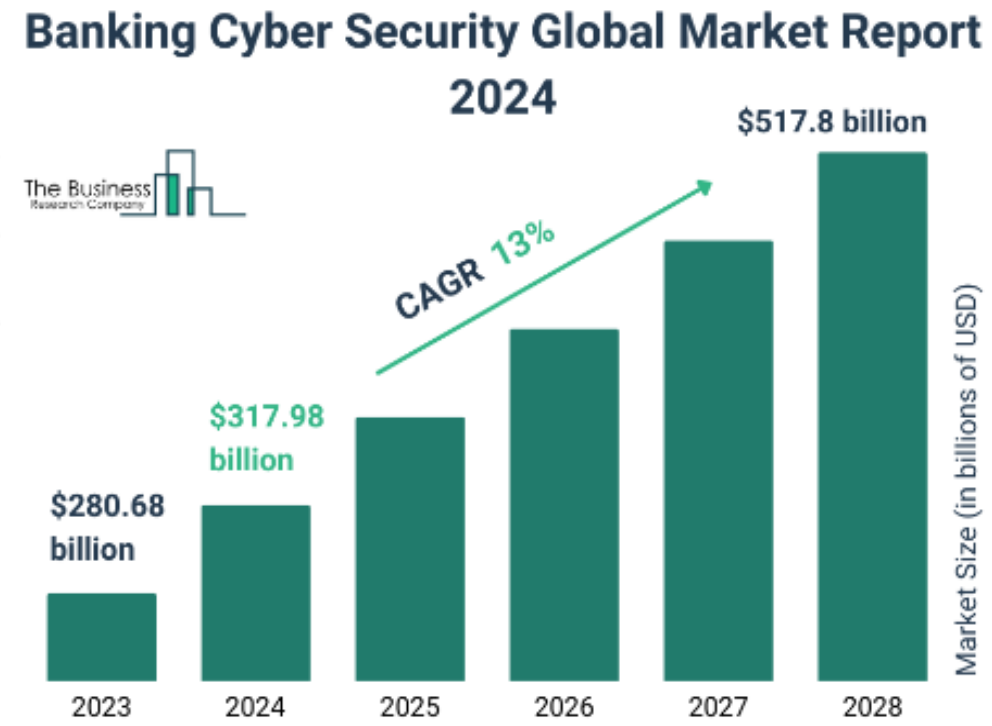
- Google Cloud Platform (GCP): GCP машиналық оқыту модельдерін құруға, оқытуға және орналастыруға арналған қуатты құралдарды ұсынады, соның ішінде TensorFlow және Vertex AI. GCP-тің үлкен деректерді өңдеу және талдау мүмкіндіктері несиелік қабілетті бағалау үшін үлкен көлемді деректерді өңдеуге және күрделі модельдерді құруға қолайлы.
- Amazon Web Services (AWS): AWS Sagemaker сияқты машиналық оқыту қызметтерін ұсынады, ол модельдерді құруды, оқытуды және орналастыруды жеңілдетеді. AWS-тің кең ауқымды деректерді сақтау және өңдеу қызметтері, сондай-ақ қауіпсіздікке бағытталған инфрақұрылымы қаржы институттары үшін маңызды.
- Microsoft Azure Machine Learning: Azure ML машиналық оқыту модельдерін әзірлеу, басқару және орналастыру үшін толыққанды платформаны ұсынады. Оның автоматтандырылған ML мүмкіндіктері және

әртүрлі интеграция нұсқалары қаржы ұйымдарына несиелік тәуекелдерді бағалауда тиімді шешімдерді құруға көмектеседі.

- IBM Watson Discovery: IBM Watson платформасы табиғи тілді өңдеу (NLP) және машиналық оқыту мүмкіндіктерін ұсынады, бұл құрылымдалмаған деректерді (мысалы, жаңалықтар, әлеуметтік медиа) талдау арқылы несиелік қабілетті бағалауға қосымша түсініктер алуға мүмкіндік береді.
- Open-source технологиялар (Python экожүйесі): Python және оның кітапханалары (Scikit-learn, TensorFlow, PyTorch, Pandas, NumPy) машиналық оқыту модельдерін әзірлеуде кеңінен қолданылады. Бұл технологиялардың икемділігі мен үлкен қоғамдастығы әртүрлі несиелік қабілетті бағалау модельдерін құруға мүмкіндік береді.

1.1.2 Банктік киберқауіпсіздік нарығына шолу

Соңғы жылдары банктік киберқауіпсіздік бизнесінің ауқымы тез кеңейді. Ол 13,3% күрделі жылдық өсу қарқынымен (CAGR) 2023 жылғы 280,68 миллиард доллардан 2024 жылы 317,98 миллиард долларға дейін өседі. Тарихи кезеңдегі өсімге тәуекелдерді басқару, киберқауіптердің күрделілігі, цифрлық трансформация, бұлттық қауіпсіздік және мобильді банкинг қауіпсіздігі жауапты. 1.1-ші суретте 2023 жылдан 2028 жылға дейінгі банк секторының киберқауіпсіздік бойынша жаһандық нарығының көлемі көрсетілген.



1.1 сурет – 2023 жылдан 2028 жылға дейінгі банк секторының киберқауіпсіздік бойынша жаһандық нарығының көлемі

Алдағы жылдары банктік киберқауіпсіздік саласының көлемі тез өседі деп күтілуде. Ол 2028 жылы 13% құрама жылдық өсу қарқынымен (CAGR) 517,8 миллиард долларға дейін өседі. Болжамдық кезеңдегі кеңею орталықтандырылмаған қаржының (DeFi) пайда болуымен, жақсартылған биометриялық аутентификациямен, жасанды интеллектті (AI) кеңейтілген пайдаланумен және кванттық есептеу тәуекелдерімен байланысты болуы мүмкін. Болжамдық кезеңде қауіпті анықтауды тереңдетіп оқыту, 5G қауіпсіздік мәселелері, цифрлық валюталар үшін киберқауіпсіздік, нөлдік күндік қауіптен қорғау, қауіпсіздікті интеллектуалды ұйымдастыру және қауіп-қатер туралы ақпаратты бірлесіп пайдалану негізгі тақырыптардың бірі болып табылады.

Банк саласындағы киберқауіпсіздік нарығының жаһандық көрсеткіштері төмендегі 1.1-ші кестеде келтірілген. Онда нарық көлемі, өсім қарқыны, жетекші аймақтар және болжамдық кезең көрсетілген.

1.1 кесте – Нарықтың көлемі мен ауқымы

Есептің қамтылуы	Мәтіні
2033 жылға дейінгі нарық көлемі	199,56 млрд АҚШ доллары
2023 жылғы нарық көлемі	57,96 млрд АҚШ доллары
2024 жылғы нарық көлемі	57,96 млрд АҚШ доллары
2024–2033 жылдардағы өсім қарқыны	Орташа жылдық өсім (CAGR) – 13,16%
Ең ірі нарық	Солтүстік Америка
Базалық жыл	2023
Болжау кезеңі	2024–2033 жж.
Қамтылған өңірлер	Солтүстік Америка, Еуропа, Азия-Тынық мұхиты, Латын Америкасы, Таяу Шығыс және Африка

1.1.3 Аймақтық салыстыру

Солтүстік Америка, әсіресе Америка Құрама Штаттары, банктік қауіпсіздік үшін маңызды нарық болып табылады. Аймақта киберқауіптердің кең таралуына және қатаң реттеуші талаптарға байланысты киберқауіпсіздік шешімдеріне көп қаржы бөлетін ірі қаржы институттары орналасқан.

Еуропа елдері, соның ішінде Ұлыбритания, Германия және Франция да банктік қауіпсіздікке қатты көңіл бөледі. Еуропалық банк секторы киберқауіпсіздік тәжірибесіне әсер ететін GDPR сияқты нормативтік базаларға бағынады.

Қытай, Жапония және Үндістан сияқты елдермен Азия-Тынық мұхиты аймағы банктік қауіпсіздікке инвестициялардың айтарлықтай өсуіне куә болуда. Қаржылық қызметтердің цифрландыруының артуы және финтехтің өркендеуі қауіпсіздіктің озық шешімдеріне сұранысқа ықпал етеді.

Латын Америкасы елдері банктік қауіпсіздікті қамтамасыз ету шараларының маңыздылығын, әсіресе цифрлық банкингті қабылдау артқан сайын мойындайды. Өңірде киберқауіпсіздік бастамалары көбірек орын алуда.

Африкадағы банктік қауіпсіздікке инвестиция деңгейі әр елде өзгереді, бірақ қаржы секторында киберқауіпсіздік шараларының қажеттілігі туралы хабардарлық өсуде. Кейбір елдер дамып келе жатқан қауіптерге қарсы тұру үшін киберқауіпсіздік мүмкіндіктерін арттыруда.

Біріккен Араб Әмірліктері мен Сауд Арабиясы сияқты Таяу Шығыстағы елдер де киберқауіптерден қорғау үшін банктік қауіпсіздікке инвестиция салуда. Аймақтың қаржы орталықтары қауіпсіздіктің озық шараларын қабылдауда.

1.1.4 Болашақтағы тенденциялар мен нарықтың болашағы

Кредиттік қабілеттілік бағалау саласында жасанды интеллект (ИИ) және машиналық оқыту (МО) технологияларының кеңінен қолданылуы болашақта маңызды рөл атқарады. Қаржы нарығындағы өзгерістер мен цифрлық трансформацияның әсерінен, кредиттік қабілеттілікті бағалау әдістері жаңарып, дәстүрлі тәсілдермен салыстырғанда әлдеқайда тиімді және дәл болмақ.

1. ИИ негізіндегі кредиттік бағалау әдістерінің кеңеюі:
Жасанды интеллектің қолданылуы арқылы кредиттік қабілеттілік бағалау анағұрлым дәл және жылдам жүзеге асырылады. ИИ жүйелері клиенттердің қаржылық тарихы, төлем қабілеттілігі, әлеуметтік және экономикалық көрсеткіштерін талдай отырып, дәстүрлі әдістерге қарағанда әлдеқайда тиімді бағалау жүргізеді. Алдағы уақытта қаржы институттары мен банктер бұл технологияларды өз қызметтерінде кеңінен қолдануды жоспарлап отыр.

2. Мәліметтерді терең талдау және болжам жасау:
Машиналық оқыту жүйелері үлкен көлемдегі деректерді талдай отырып, клиенттің кредиттік қабілеттілігі туралы дәлірек болжамдар жасауға мүмкіндік береді. ИИ моделдері тек қана қаржылық көрсеткіштерді емес, сондай-ақ тұтынушының әлеуметтік тәртібі, төлем тарихы, тіпті мобильді қолдану мен интернеттегі белсенділігі сияқты факторларды да ескеріп, несиелік қабілеттілікті бағалай алады.

3. Кредиттік тәуекелдерді болжау және басқару:
ИИ мен МО қаржы ұйымдарына несиелік тәуекелдерді дәл болжауға және оларды басқаруға мүмкіндік береді. Бұл технологиялар клиенттерді жоғары тәуекел топтарына бөлуге, тәуекелдер бойынша алдын ала ескертулер жасауға және несие беру шешімдерін тиімдірек қабылдауға көмектеседі. Бұл, өз кезегінде, қаржылық ұйымдардың шығындарын азайтуға және клиенттермен жұмыс істеу тиімділігін арттыруға мүмкіндік береді.

4. Қаржылық инклюзияның артуы:
ИИ мен МО негізіндегі жүйелер арқылы дәстүрлі несие тарихы жоқ немесе жеткіліксіз ақпаратпен қамтылған клиенттерге несие беру мүмкіндігі артады.

Бұл қаржылық инклюзияны арттырып, көбірек адамдарға банктік қызметтерге қолжетімділікті қамтамасыз етеді.

5. Құқықтық және этикалық мәселелер:
ИИ негізіндегі кредиттік қабілеттілікті бағалау әдістері заңды және этикалық мәселелерді де көтереді. Қаржы ұйымдары бұл технологияларды енгізгенде, пайдаланушылардың деректерінің құпиялығын сақтауды және әділ шешімдер қабылдауды қамтамасыз етуі қажет. Болашақта осы мәселелерді шешу үшін тиісті реттеу шаралары мен стандарттар әзірленуі мүмкін.

Жалпы алғанда, ИИ және МО технологияларының қолданылуы кредиттік қабілеттілікті бағалауды анағұрлым дәл, әділ және тиімді етеді. Алдағы жылдары бұл саланың болашағы зор болып, жаңа мүмкіндіктер мен инновациялар енгізілуі күтілуде.

1.2 Барлық аналогтардың салыстырмалы талдауы

Кредиттік қабілеттілікті бағалау саласында бірнеше бар әдістер мен жүйелер қаржы ұйымдары тарапынан жеке тұлғалар мен кәсіпорындардың несие қабілеттілігін бағалау үшін қолданылып келеді. Бұл әдістер уақыт өте келе дамып, қаржылық есептемелерге негізделген дәстүрлі бағалаудан, қазіргі заманғы жасанды интеллект (ИИ) және машиналық оқыту (МО) технологияларын қолдануға ауысты. Төменде дәстүрлі кредиттік балл жүйелері мен қазіргі ИИ-негізіндегі шешімдерді салыстырмалы талдау берілген.

1. Дәстүрлі кредиттік балл жүйелері

Дәстүрлі кредиттік балл жүйелері, мысалы, FICO баллы мен VantageScore, банктер мен қаржы ұйымдарында несие қабілеттілігін бағалауда кеңінен қолданылды. Бұл модельдер көбінесе келесі факторларға негізделеді:

- Қарызды төлеу тарихы (несие карталары мен қарыздар бойынша төлемдер).
- Қарыздың көлемі (қарыздардың жалпы мөлшері).
- Несие тарихының ұзақтығы (кредиттік шоттың ашылған уақыты).
- Жаңа несиелердің саны (несие карточкалары немесе басқа қарыз түрлерінің ашылуы).
- Қаржылық деректердің түрлері (жалақы, банктік шоттар).

Бұл жүйелердің негізгі кемшілігі — олар тек қаржылық ақпаратты ескеріп, қарыз алушының әлеуметтік немесе мінез-құлықтық факторларын елемейді. Сонымен қатар, дәстүрлі әдістер жоғары тәуекелді және несие тарихы жоқ тұлғаларды бағалауда шектеулерге ие.

2. ИИ-негізіндегі кредиттік қабілеттілікті бағалау жүйелері

Жасанды интеллект және машиналық оқыту негізіндегі жаңа шешімдер дәстүрлі жүйелердің шектеулерін жеңуге мүмкіндік береді. Бұл әдістер көптеген қосымша деректер көздерін пайдалана отырып, әлдеқайда толық және дәлірек бағалауды қамтамасыз етеді. ИИ жүйелері келесі мүмкіндіктерді ұсынады:

- Қаржылық емес деректерді ескеру**:** ИИ жүйелері тек қаржылық ақпаратпен шектелмей, тұтынушының әлеуметтік медиа белсенділігін, мінез-құлықтық үлгілерін және басқа да қосымша деректерді талдайды.
- Жоғары дәлдік**:** Машиналық оқыту алгоритмдері үлкен деректерді өңдеп, күрделі байланыстарды анықтап, тәуекелдерді жақсырақ болжайды.
- Динамикалық шешімдер қабылдау**:** ИИ жүйелері уақыт өте келе оқып, жетілдіріледі, бұл олардың болжамдарын үнемі жақсартады.
- Тәуекелді бағалаудың кең ауқымы**:** Бұл әдістер дәстүрлі балл жүйелеріне қарағанда неғұрлым көп факторларды ескереді, соның ішінде тұтынушының жеке мінез-құлқынан бастап, сыртқы экономикалық факторларға дейін.

1.2.1 Қауіпсіздік деңгейі

Кредиттік қабілеттілікті бағалау жүйелерінің қауіпсіздік деңгейі — бұл жүйенің сыртқы және ішкі қауіптерден, соның ішінде деректердің заңсыз қол жеткізілуінен, бұзылуынан немесе бұрмалануынан қаншалықты қорғалғанын білдіретін маңызды көрсеткіш. Әсіресе жасанды интеллектке негізделген жүйелер үлкен көлемдегі жеке және қаржылық ақпаратты өңдейтін болғандықтан, олардың қауіпсіздігі басты назарда болуы тиіс.

Дәстүрлі жүйелердегі қауіпсіздік

Дәстүрлі несие скоринг жүйелері әдетте орталықтандырылған деректер базасына сүйенеді. Бұл жүйелерде мынандай қауіпсіздік тәуекелдері жиі кездеседі:

- Құпия деректердің ұрлануы**:** Әсіресе егер жүйе ескі шифрлау технологияларын қолданса.
- Фишинг шабуылдарына бейімділік**:** Қолданушылардың логин/пароль жүйесі арқылы жүйеге кіруі фишинг секілді шабуыл түрлеріне осал етеді.
- Бірегей аутентификацияның болмауы**:** Қарапайым логин мен құпия сөз арқылы кіру жеткілікті болуы мүмкін.

ИИ-негізіндегі жүйелердегі қауіпсіздік

Жасанды интеллект пен машиналық оқыту негізіндегі жүйелер, әдетте, заманауи қауіпсіздік стандарттарына сай құрылады. Олардың қауіпсіздік артықшылықтарына мыналар жатады:

- Мәліметтерді шифрлау**:** Деректер тасымалдану және сақтау барысында AES-256 секілді заманауи алгоритмдермен шифрланады.
- Көп факторлы аутентификация (MFA)**:** Жүйеге кіру тек логин/құпия сөз арқылы ғана емес, сонымен қатар биометрикалық немесе SMS/Email растау арқылы жүзеге асады.
- Қолданушылар әрекетін бақылау**:** ИИ жүйелері күдікті әрекеттерді автоматты түрде анықтап, алдын ала шаралар қолданады.

- Қауіп-қатерлерді алдын ала болжау**:** Машиналық оқыту арқылы жүйе ықтимал шабуылдарды немесе аномалияларды алдын ала болжап, әрекет ете алады.

1.2.2 Қолданылуы

Пайдаланушылық ыңғайлылығы — кез келген жүйенің, соның ішінде кредиттік қабілеттілікті бағалау жүйелерінің сәтті жұмыс істеуінің маңызды аспектілерінің бірі. Бұл көрсеткіш жүйені қолданушының оңай, тез әрі интуитивті түрде пайдалана алу қабілетін сипаттайды. Егер жүйе күрделі, түсініксіз немесе тым техникалық болса, тіпті ең қауіпсіз және дәл жүйе де пайдаланушы тарапынан қабылданбауы мүмкін.

1. Дәстүрлі жүйелердегі пайдаланушылық.

Дәстүрлі кредиттік скоринг жүйелерінде пайдаланушы тәжірибесі көбінесе екінші орында тұрады. Мұндай жүйелердің кейбір сипаттамалары:

- Интерфейс қарапайым, бірақ ескі дизайнда болуы мүмкін.
- Қолмен дерек енгізу қажет — бұл қате жіберуге және уақыт жоғалтуға әкеледі.
- Кері байланыс баяу — пайдаланушы нәтижені бірнеше күн күтуі мүмкін.

2. ИИ-негізіндегі жүйелердегі пайдаланушылық.

Жасанды интеллектке негізделген жүйелерде пайдаланушылық тәжірибеге ерекше мән беріледі. Мұндай жүйелерде келесі артықшылықтар бар:

- Интуитивті интерфейс — заманауи UX/UI шешімдері арқасында қолдану оңай.
- Автоматтандырылған дерек жинау — пайдаланушыдан минималды әрекет талап етіледі.
- Жылдам нәтиже — жүйе бірнеше секундта скоринг нәтижесін ұсына алады.
- Мобильді құрылғыларға бейімделген — қосымшалар мен сайттар смартфонға ыңғайлы.

Қазіргі таңда несиелік қабілеттілікті бағалау жүйелері технологиялық дамуымен тығыз байланысты. Дәстүрлі әдістер ұзақ уақыт бойы банктік және қаржылық ұйымдарда кеңінен қолданылып келсе де, олардың дәлдігі мен тиімділігі шектеулі. Ал жасанды интеллект негізіндегі жүйелер бұл бағытта едәуір артықшылықтар ұсынуда. Мұндай жүйелер үлкен көлемдегі деректерді өңдеу, тәуекелдерді алдын ала болжау және пайдаланушы тәжірибесін оңтайландыру арқылы шешім қабылдаудың сапасын арттырады.

Төменде келтірілген 1.2-ші кестеде дәстүрлі және ИИ-негізіндегі жүйелер арасындағы негізгі айырмашылықтар бірқатар көрсеткіштер бойынша салыстырылып берілген. Бұл салыстырмалы талдау заманауи тәсілдердің артықшылықтарын жүйелі түрде көрсетуге және тиімділігін негіздеуге мүмкіндік береді. Ол сонымен қатар жүйені таңдаудағы стратегияны айқындауға көмектеседі.

1.2 кесте - Дәстүрлі және ИИ-негізіндегі жүйелер арасын салыстырылып талдау

Көрсеткіш	Дәстүрлі жүйе	ИИ-негізіндегі жүйе
Интерфейс заманауилығы	Орташа немесе төмен	Жоғары
Қолданудың жеңілдігі	Орташа	Өте жоғары
Жауап алу жылдамдығы	Баяу (бірнеше сағат/күн)	Жылдам (бірнеше секунд/минут)
Пайдаланушы қатысуы	Көп (қолмен енгізу)	Аз (автоматтандырылған процестер)

Жасанды интеллектке негізделген жүйелер тек дәлдік пен қауіпсіздік бойынша ғана емес, пайдаланушылық ыңғайлылығы жағынан да дәстүрлі тәсілдерден басым. Мұндай жүйелер банк клиенттеріне ыңғайлы, жылдам әрі оңай жолмен қаржылық бағалау жүргізуге мүмкіндік береді. Бұл өз кезегінде банктердің де клиентпен байланысын нығайтып, қызмет сапасын арттырады.

1.2.3 Интеграция

Жүйенің масштабталуы мен интеграция мүмкіндігі — қазіргі заманғы қаржы технологияларында, әсіресе жасанды интеллектке негізделген кредиттік скоринг жүйелерінде маңызды рөл атқаратын факторлар. Бұл бөлімде жүйенің кеңеюі мен түрлі платформалармен бірігіп жұмыс істеу қабілеттері қарастырылады.

1. Масштабталу (Scalability)

Масштабталу — жүйенің жүктеме артқанда да тұрақты әрі тиімді жұмыс істеу қабілеті. Жүйе қолданушылар саны артқан сайын немесе өңделетін мәлімет көлемі ұлғайғанда өнімділікті төмендетпей жұмыс істеуі қажет.

2. Дәстүрлі жүйелердің шектеулері:

- Көбінесе локалдық серверлерге негізделген;
- Жоғары жүктеме кезінде баяулайды;
- Жаңа функцияларды қосу үшін көп уақыт пен шығын қажет.

3. ИИ-негізіндегі жүйелердің артықшылықтары:

- Бұлтты технологияларды қолдану арқылы масштабталу жеңіл;
- Көптеген пайдаланушыға бір уақытта қызмет көрсете алады;
- Автоматтандырылған процестер арқылы жүйе өзін-өзі оңтайландырады.

4. Интеграция (Integration)

Интеграция — жүйенің басқа бағдарламалармен, платформалармен немесе деректер қорларымен үйлесімді жұмыс істеу мүмкіндігі. Бұл кредиттік қабілеттілікті бағалау жүйесін банктің ішкі жүйелерімен, CRM, ERP немесе басқа қаржы платформаларымен байланыстыруда маңызды.

5. Дәстүрлі жүйелер:

- Интеграцияны қолмен жасау қажет;
- API интерфейстері жиі шектеулі немесе ескі;
- Басқа жүйелермен біріктіру көп еңбекті талап етеді.

6. ИИ-негізіндегі жүйелер:
- Ашық және құжатталған API-лерді ұсынады;
- Басқа платформалармен тез біріктіріледі (мысалы, Open Banking жүйелерімен);
- Реал-тайм деректер алмасуға мүмкіндік береді.

1.2.4 Қауіптерге бейімделу қабілеті

Қаржы секторы үнемі өзгеріп отыратын киберқауіптерге тап болып отырады. Осыған байланысты, жүйенің қауіптерге бейімделу қабілеті — кредиттік қабілеттілікті бағалау жүйесінің сенімділігі мен ұзақмерзімді тиімділігінің басты көрсеткіштерінің бірі болып саналады.

1. Дәстүрлі жүйелердің әлсіз тұстары:
- Қауіптерді алдын ала болжау және бейімделу қабілеті шектеулі;
- Шабуылдарға жауап беру процесі көбіне қолмен іске асады;
- Жаңа қауіп түрлері пайда болғанда жүйені жаңарту кешіктіріледі.

2. ИИ-негізіндегі жүйелердің артықшылықтары:
- Машина оқыту алгоритмдері арқасында шабуыл үлгілерін анықтай алады;
- Аномалияларды автоматты түрде бақылау арқылы күдікті әрекеттерді ерте кезеңде таниды;
- Қауіптердің эволюциясына бейімделіп, жүйе өзін-өзі жетілдіре алады.

3. Қауіптерге жауап беру әдістері:
- Аномалияларды анықтау: ИИ жүйесі қалыпты мінез-құлықтан ауытқуларды тіркеп, бірден әрекет етеді.
- Үздіксіз оқыту: Жүйе жаңа деректерге сүйене отырып, қауіп-қатерлерді тану қабілетін үздіксіз жетілдіреді.
- Реал-тайм бақылау: Уақытында ескерту және шабуылға қарсы жылдам әрекет жасау мүмкіндігі.

1.2.5 Банктік инфрақұрылыммен интеграция

Кредиттік қабілеттілікті бағалауға арналған жүйелердің банктік инфрақұрылыммен үйлесімді интеграциялануы — олардың табысты іске асырылуы мен тиімді жұмыс істеуінің негізгі шарты. Интеграцияның сәтті өтуі банк жүйелерінің үздіксіздігін, қауіпсіздігін және деректердің біртұтастығын қамтамасыз етеді.

1. Дәстүрлі жүйелер:
- Жиі дербес жұмыс істейді**,** банктің негізгі жүйелерімен интеграциясы шектеулі;

- Интеграция процесі көп уақыт пен ресурсты қажет етеді;
- Көбінесе қолмен енгізілетін деректерге сүйенеді, бұл қателіктерге жол ашады.

2. ЖИ-негізіндегі жүйелер:

- API арқылы интеграциялау мүмкіндігі бар**,** бұл деректер алмасуды автоматтандыруға мүмкіндік береді;
- Нақты уақыт режимінде банк жүйелерінен клиенттік ақпаратты ала алады;
- Заманауи банк платформаларына оңай бейімделеді (мысалы, CRM, ERP, Core Banking жүйелерімен үйлесімді).

3. Интеграция артықшылықтары:

- Автоматтандыру: Қолмен енгізуді азайтып, адам факторынан болатын қателерді жояды;
- Жедел шешім қабылдау: Нақты уақыттағы деректердің негізінде несие беру шешімін жедел қабылдауға көмектеседі;
- Масштабталу: Банк инфрақұрылымының кеңеюіне қарай ИИ жүйесі де оңай бейімделеді;
- Қауіпсіздік: Интеграция кезінде шифрлау және қол жеткізу деңгейін бақылау сынды қауіпсіздік шаралары қолданылады.

ИИ негізінде жасалған жүйелер банктік инфрақұрылыммен икемді әрі қауіпсіз интеграциялануы арқылы процестерді автоматтандырып, шешім қабылдау сапасын арттырады. Бұл банктерге ішкі тиімділікті жоғарылатып қана қоймай, клиенттерге де жылдам әрі сапалы қызмет көрсетуге мүмкіндік береді.

1.2.6 Банктік инфрақұрылы қорытынды

Жобаның тақырыбы — "Жасанды интеллект негізінде кредиттік қабілеттілікті бағалау жүйесін әзірлеу" — қазіргі қаржы нарығы үшін аса өзекті. Цифрлық технологиялардың, соның ішінде жасанды интеллекттің дамуы банктік қызметтерді автоматтандыру мен жедел шешім қабылдауға жаңа мүмкіндіктер ашуда.

Аналитикалық бөлімде біз нарықтағы қазіргі жүйелерді зерттеп, олардың қауіпсіздік деңгейін, пайдалануға ыңғайлылығын, ауқымдылығын және банктік инфрақұрылыммен интеграциялану мүмкіндіктерін талдадық. Зерттеу нәтижесі көрсеткендей, дәстүрлі әдістердің мүмкіндіктері шектеулі және олар қазіргі заманғы киберқауіптерге төтеп бере алмайды. Ал жасанды интеллектке негізделген жүйелер:

- неғұрлым дәл әрі объективті шешімдер қабылдауға,
- клиенттер туралы үлкен көлемдегі деректерді өңдеуге,
- операцияларды автоматтандыру арқылы банктің тиімділігін арттыруға мүмкіндік береді.

Сонымен қатар, ИИ жүйелерінің банктік инфрақұрылыммен жеңіл интеграциялануы — оларды нақты жағдайда қолдануға тиімді етеді. Бұл жобаның нәтижесі ретінде ұсынылатын ИИ жүйесі банктер үшін тек қауіпсіздік

пен тиімділік құралын ғана емес, сонымен қатар клиентке бағдарланған заманауи шешім бола алады.

1.3 Жобаның сипаттамасы

Бұл жобаның негізгі мақсаты – жасанды интеллект негізінде кредиттік қабілеттілікті бағалау жүйесін әзірлеу. Жобада дәстүрлі әдістердің кемшіліктерін жоюға және шешім қабылдауды автоматтандыруға бағытталған заманауи технологиялар қолданылады.

Жобада төмендегідей негізгі міндеттер қарастырылған:

- Клиент туралы деректерді жинау және өңдеу: пайдаланушының төлем қабілеттілігіне әсер ететін деректерді (жалақы, шығындар, кредиттік тарих, әлеуметтік мінез-құлық т.б.) жинау;
- Машинамен оқыту модельдерін қолдану: логистикалық регрессия, шешім ағаштары, нейрондық желілер және басқа алгоритмдер арқылы клиенттің кредиттік тәуекелін болжау;
- Бағалау нәтижелерін визуализациялау: банктің кредит беру бөлімінің мамандары үшін интуитивті және түсінікті аналитикалық интерфейс құру;
- Қауіпсіздік және деректерді қорғау: жеке деректерді сақтау және өңдеу кезінде қауіпсіздік талаптарын сақтау;
- Банктік инфрақұрылыммен интеграция: жүйені бар ақпараттық жүйелермен біріктіру арқылы деректер алмасуды жеңілдету.

Жоба Python, PostgreSQL және React сияқты заманауи технологиялар негізінде әзірленеді. Python – мәліметтерді өңдеу және машиналық оқыту модельдерін құру үшін, PostgreSQL – құрылымдалған деректер базасын басқару үшін, ал React – қолданушы интерфейсін құру үшін пайдаланылады.

Нәтижесінде бұл жүйе банктерге клиенттің қаржылық сенімділігін жылдам әрі дәл бағалауға көмектесіп, кредиттік тәуекелдерді азайтуға және шешім қабылдау процесін оңтайландыруға мүмкіндік береді.

1.3.1 Жобаның мақсаттары

Жобаның мақсаты – жасанды интеллект технологияларын пайдалана отырып, банктік клиенттердің кредиттік қабілеттілігін дәл әрі тиімді бағалауға мүмкіндік беретін қауіпсіз және интеллектуалды жүйе әзірлеу.

Жобаның негізгі міндеттері:

1. Ақпарат жинау жүйесін әзірлеу: Клиент туралы қаржылық, әлеуметтік және мінез-құлықтық деректерді жинау мен сақтау тетігін құру.
2. Машинамен оқыту моделін жасау: Кредиттік тәуекелді болжау үшін машиналық оқыту алгоритмдерін (мысалы, логистикалық регрессия, шешім ағаштары, нейрондық желілер) қолдану.

3. Деректерді өңдеу және алдын ала талдау: Модель сапасын арттыру үшін деректерді тазарту, түрлендіру және талдау құралдарын енгізу.

4. Жүйенің қауіпсіздігін қамтамасыз ету: Пайдаланушының жеке және қаржылық деректерін сақтау кезінде қауіпсіздік талаптарын сақтау.

5. Қолданушы интерфейсін әзірлеу: Банктің қызметкерлері үшін оңай қолданылатын және деректерге негізделген шешім қабылдауға мүмкіндік беретін веб-интерфейс жасау.

6. Банктік инфрақұрылыммен интеграция: Жүйені банктің ішкі ақпараттық жүйелерімен біріктіру арқылы автоматтандырылған және тиімді жұмыс істеуді қамтамасыз ету.

Бұл міндеттер жобаның нақты әрі қолжетімді нәтижелерге бағытталғанын көрсетеді және банктерге клиенттердің кредиттік қабілеттілігін бағалауда заманауи шешім ұсынады.

1.3.2 Сұраныстармен жұмыс істеу принципі тіркеу мысалы негізінде қарастырылады

1. Пайдаланушы:

• Пайдаланушы қолданбамен әрекеттесуді бастайды, мысалы, веб-интерфейс арқылы сұрау жіберу.

2. Тіркеу:

• Сұранысты өңдеудің бірінші кезеңі. Бұл пайдаланушы тіркеу мәліметтерін енгізетін пішін немесе соңғы нүкте болуы мүмкін.

• Бұл жерде енгізілген деректерді жинау және алдын ала тексеру жүргізіледі.

3. Контроллер (контроллер):

• Контроллер пайдаланушының сұрауын қабылдайды (мысалы, тіркеуге арналған POST сұрауы).

• Ол HTTP сұрауларын өңдейді, кіріс деректерді басқарады және жауаптарды жасайды.

• Контроллер деректерді одан әрі өңдеу үшін қызмет көрсету деңгейінің сәйкес әдістерін шақырады.

4. Қызмет:

• Қызметтік деңгей қолданбаның іскери логикасын қамтиды. Бұл қабатта негізгі деректерді өңдеу орын алады, мысалы, пайдаланушының бірегейлігін тексеру, парольдерді шифрлау және т.б.

• Іскерлік ережелердің орындалуын қамтамасыз ете отырып, контроллер мен репозиторий арасындағы делдал қызметін атқарады.

5. Репозиторий:

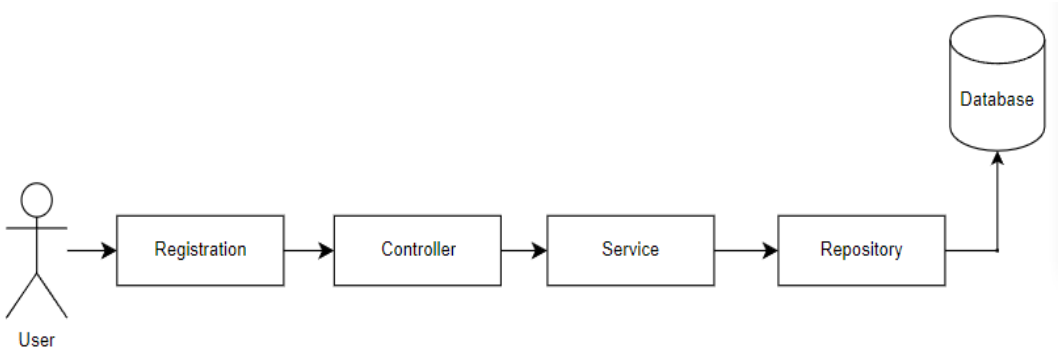
• Репозиторий дерекқормен өзара әрекеттесуге жауапты. Бұл деректерді сақтау, шығарып алу, жаңарту және жою әдістерін қамтамасыз ететін деректердің абстракциясы.

• Django REST бағдарламасында, мысалы, репозиторийлер Spring автоматты түрде жүзеге асыратын интерфейс болуы мүмкін.

6. Мәліметтер қоры:

• Бұл барлық қолданба деректері сақталатын орын. Репозиторий мәліметтер базасында жаңа пайдаланушыны сақтау, сұраныстар бойынша деректерді алу және т.б. сияқты операцияларды орындайды.

Ақпараттық жүйелерде пайдаланушы сұранысын өңдеу белгілі бір архитектуралық құрылымға сүйеніп жүзеге асырылады. Бұл құрылым жүйенің әр компонентінің нақты міндетін анықтап, модульдер арасындағы байланысты көрсетеді. Төмендегі 1.2-ші суретте көрсетілген диаграммада пайдаланушы тіркелген кезде сұраныстың қалай өңделетіні көрсетілген. Бұл процесс MVC (Model-View-Controller) және Service-Repository архитектуралық үлгілері негізінде құрастырылған.



1.2 сурет – Тіркеу мысалында сұраныстармен жұмыс істеу принципі

Суретте көрсетілгендей, пайдаланушы Registration интерфейсі арқылы жүйеге сұраныс жібереді. Бұл сұраныс Controller модуліне бағытталып, онда өңделіп, логиканы орындау үшін Service қабатына беріледі. Service қажетті операцияларды орындайды және деректермен жұмыс істеу үшін Repository қабатына жүгінеді. Repository өз кезегінде деректер қорымен байланысады және нәтижені қайтарады. Мұндай құрылым жүйенің модульдік сипатын сақтай отырып, кеңейту мен тестілеуді жеңілдетеді.

1.3.3 Жобаның негізгі құрамдас бөліктері

1. Аутентификация және авторизация.

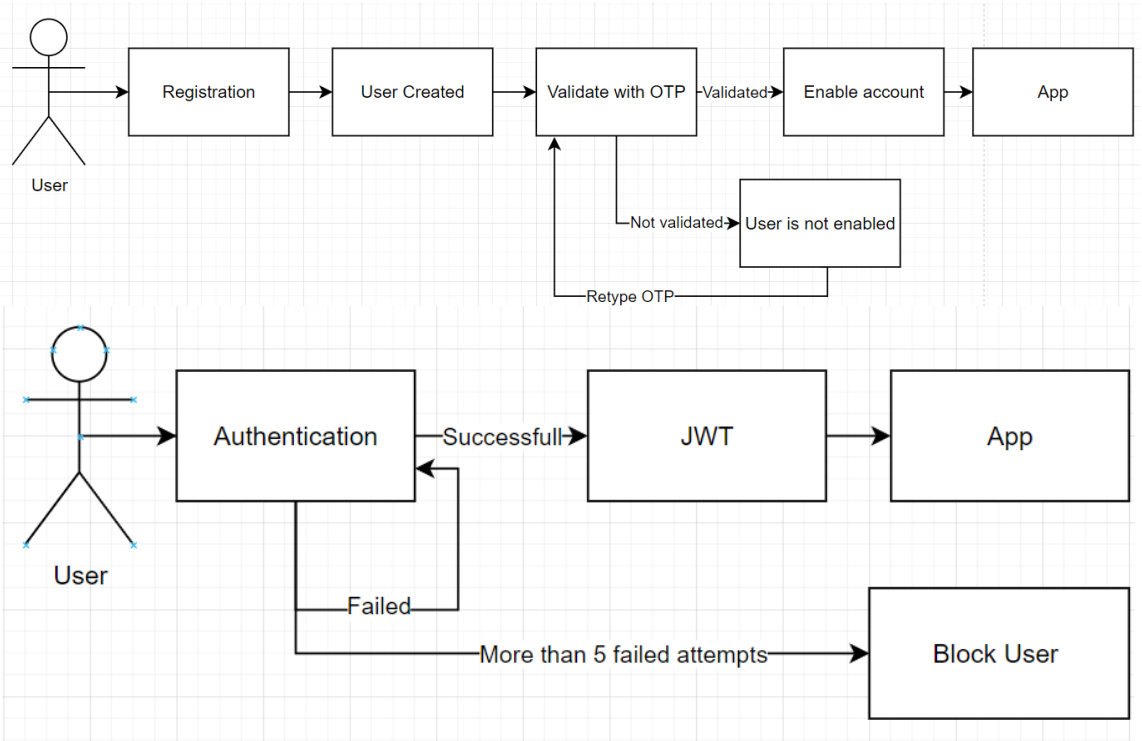
Жүйе пайдаланушы аты мен құпия сөз сияқты дәстүрлі әдістерді көп факторлы аутентификация (MFA) сияқты озық әдістермен үздіксіз үйлестіре отырып, аутентификацияға көп деңгейлі тәсілді қолданады. Пайдаланушылар өздерінің жеке басын бірнеше факторлар арқылы растауы керек, олар білетін нәрсе (құпия сөз), оларда бар нәрсе (қауіпсіздік белгісі) және олар (биометриялық деректер) болып табылады. Саусақ ізі және бет-әлпетті тану сияқты биометриялық аутентификация опцияларын қосу арқылы жүйе

қауіпсіздікті жақсартады, сонымен бірге пайдаланушының үздіксіз және интуитивті тәжірибесін қамтамасыз етеді. Бұған қоса, мінез-құлық талдаулары пайдаланушы әрекетінің үлгілерін бақылау және рұқсатсыз кіру әрекеттерін көрсетуі мүмкін бейтаныс орындардан немесе құрылғылардан кірулер сияқты ауытқуларды анықтау үшін құрылымға біріктірілген. Аутентификацияның бұл кешенді тәсілі жүйенің көптеген ықтимал қауіптерді өңдеу үшін жабдықталғанын қамтамасыз етеді.

Рөлге негізделген қатынасты басқару (RBAC) бойынша авторизациялау механизмі пайдаланушыларға олардың нақты рөлдеріне сәйкес ресурстар мен функцияларға ғана рұқсат беруін қамтамасыз ететіндей жасалған. Бұл бұзылған шоттың ықтимал әсерін айтарлықтай азайтады және рұқсаттарды басқаруға құрылымдық және ұйымдастырылған тәсілді ұсынады, осылайша онлайн-банкинг қолданбасының жалпы қауіпсіздігін арттырады.

Ақпараттық жүйеде пайдаланушыны тіркеу және жүйеге кіру (аутентификация) қауіпсіздіктің маңызды құрамдас бөліктері болып табылады. Бұл кезеңдер жүйеге рұқсат алу құқығы бар нақты тұлғаны анықтау үшін қажет. Пайдаланушының тіркеуі тек бір реттік құпия кодпен (OTP) расталғаннан кейін ғана есептік жазбаны іске қосуға мүмкіндік береді. Ал аутентификация кезеңінде жүйе пайдаланушының дұрыс мәлімет енгізгенін тексереді, және бірнеше рет сәтсіз әрекеттер болған жағдайда қауіпсіздік шараларын қолданады.

Төмендегі 1.3, 1.4-ші суреттерде көрсетілген диаграммаларда осы екі процестің визуалды түрде қалай жүзеге асырылатыны көрсетілген.



1.3, 1.4 сурет – Тіркеу және аутентификация процестерінің визуалды көрінісі

2. Технологиялық стек.

Бұл жоба үшін таңдалған технологиялық стек жоғары өнімділікті, қауіпсіздікті және ауқымдылықты қамтамасыз ету үшін мұқият әзірленген, осылайша бастаманың өршіл мақсаттарын қолдайды:

- Django: бұл Python негізіндегі құрылым аутентификация сүзгілері мен рөлге негізделген қол жеткізуді басқару механизмдерін қоса, сенімді кірістірілген қауіпсіздік мүмкіндіктерін қамтамасыз ете отырып, микросервистердің дамуын жеңілдетуде маңызды рөл атқарады. Оның дизайны дерекқорлармен және басқа қызметтермен интеграцияны жеңілдетеді, бұл оны сенімділік пен қауіпсіздіктің жоғары деңгейін талап ететін қауіпсіз веб-қосымшалар үшін тамаша таңдау жасайды.

- PostgreSQL: сенімді, ашық бастапқы дерекқор жүйесі ретінде PostgreSQL күрделі сұраулар мен ACID транзакцияларын қолдайды, бұл деректердің тұтастығы мен сенімділігін қамтамасыз етеді. Оның кірістірілген шифрлау қолдауы оны деректер қауіпсіздігі маңызды болып табылатын банктік қолданбалар үшін қолайлы таңдау жасайды.

- NGINX және Google Cloud Platform (GCP): NGINX қолданбаның жауаптылығы мен сенімділігін арттыра отырып, өнімділігі жоғары жүктеме теңестіруші және веб-сервер ретінде қызмет етеді. GCP мүмкіндігін пайдалана отырып, жоба деректерді сақтау, талдау және машиналық оқыту қызметтерін ұсынатын қауіпсіз бұлттық инфрақұрылымның пайдасын көреді, олардың барлығы ықтимал қауіптерді тиімді анықтау және оларға жауап беру үшін пайдалануға болады.

Қауіпсіздік мүмкіндіктері және енгізу

1. Көп факторлы аутентификация (MFA): Бұл маңызды мүмкіндік пайдаланушылардан электрондық пошта немесе SMS арқылы жеткізілетін бір реттік құпия сөздер (OTP) немесе тексеру үшін QR кодтарын пайдалану арқылы жеке басын растауды талап ету арқылы қауіпсіздіктің маңызды деңгейін қосады. Бұл құпия сөздің ағып кетуі жағдайында есептік жазбаның бұзылу қаупін айтарлықтай төмендетеді, бұл оны қауіпсіздік жүйесінің негізгі құрамдас бөлігі етеді.

Бұл іске асырудың жұмыс схемасы келесідей:

1. Пайдаланушы қауіпсіздік параметрлерінде CIM қосады

2. Келесі пайдаланушы аутентификация әрекетінде бағдарлама алдымен пайдаланушы аты мен құпия сөзді сұрап, олардың дұрыстығын тексеруі керек.

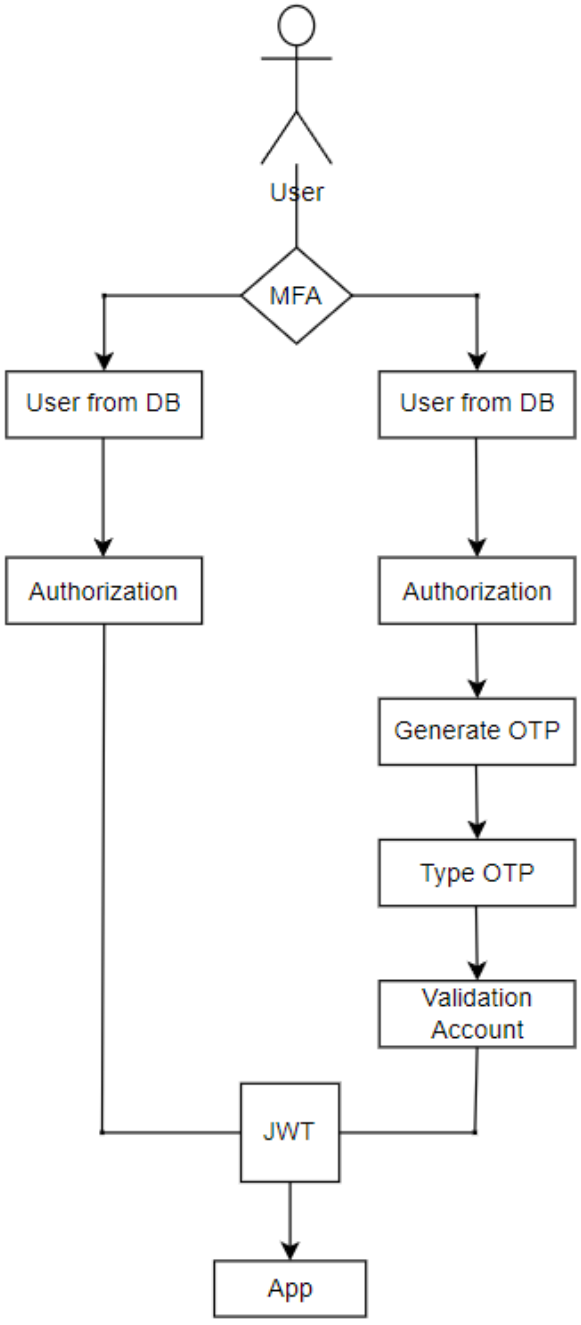
3. Тексеруден кейін пайдаланушы аты мен құпия сөздің екеуі де дұрыс болса, бағдарлама кездейсоқ бір реттік кодты жасайды және оны пайдаланушының электрондық поштасына жібереді.

4. Пайдаланушы поштаға жіберілген кодты енгізеді және бағдарлама оның дұрыстығын тексереді.

5. Егер код пен пайдаланушы деректері дұрыс болса, бағдарлама Access және Refresh таңбалауыштарын жасайды және пайдаланушыға қолданбаға кіруге мүмкіндік береді.

Ақпараттық қауіпсіздікті арттыру мақсатында көптеген заманауи жүйелер көпфакторлы аутентификацияны (MFA – Multi-Factor Authentication) қолданады. Бұл әдіс пайдаланушының тек логин мен құпиясөз арқылы емес, сонымен қатар қосымша растау факторын енгізу арқылы жүйеге кіруін талап етеді. Мұндай тәсіл шабуылдардың алдын алу және рұқсат етілмеген қолжетімділікті болдырмау үшін өте тиімді.

Төменде 1.5-ші суретте көрсетілген диаграммада көпфакторлы аутентификация процесінің жалпы архитектурасы сипатталған.



1.5 сурет – MFA жүзеге асыру жүйесі

Диаграмма екі сценарийді көрсетеді: пайдаланушы бірден дерекқор арқылы тексеруден өтіп авторизацияланса, екінші сценарийде оған бір реттік құпия код (OTP) жіберіледі. Пайдаланушы бұл кодты енгізген соң жүйе оның тіркелгісін растайды. Екі жағдайда да соңғы қадам – JWT токенін генерациялау және қосымшаға (App) қолжетімділік беру болып табылады. Бұл әдіс жүйенің сенімділігі мен қауіпсіздігін едәуір арттырады.

2 Теориялық бөлім

Бұл бөлімде онлайн-банкингтің аутентификация және авторизация жүйесінің теориялық негіздері мен архитектурасы көрсетілген. Ол негізгі компоненттер мен олардың өзара әрекеттесуін сипаттайтын жүйе архитектурасына шолу жасаудан басталады. Әрі қарай, деректердің тұтастығы мен сенімділігін қамтамасыз ету үшін қолданылатын қауіпсіздік механизмдеріне назар аудара отырып, қорғау жүйесі егжей-тегжейлі.

ER диаграммасы пайдаланушылар, тіркелгілер және транзакциялар сияқты негізгі нысандар арасындағы қарым-қатынастарды бөлектей отырып, дерекқор құрылымын суреттейді. Бөлім сонымен қатар қазіргі аутентификация әдістерін, соның ішінде көп факторлы аутентификацияны (MFA), биометрияны және мінез-құлық талдауын қамтиды, олардың дәстүрлі құпия сөзге негізделген жүйелермен салыстырғанда қауіпсіздікті арттырудағы рөлін түсіндіреді. Соңында, жоба киберқауіпсіздіктің озық тәжірибелеріне сәйкестікті қамтамасыз ету үшін тиісті қауіпсіздік хаттамалары мен салалық стандарттарды талқылайды. Бұл іргелі тұжырымдамалар жүйені жобалау мен енгізуге бағыт береді, онлайн-банкинг үшін қауіпсіз және тиімді шешімді қамтамасыз етеді.

2.1 Жобаның жалпы архитектурасы

• Пайдаланушылар (Клиенттер) → Веб немесе мобильді қолданбалар арқылы жүйемен әрекеттесетін соңғы пайдаланушыларды көрсетіңіз.

• Frontend (UI Layer) → React, Angular немесе пайдаланушының өзара әрекеттесуі үшін пайдаланылатын кез келген алдыңғы технология.

• Backend (API деңгейі) → Аутентификация және авторизация қызметі (мысалы, Spring Boot, Django, т.б.).

• Деректер қоры (сақтау деңгейі) → PostgreSQL, MySQL немесе пайдаланушы деректері мен рөлдеріне арналған басқа дерекқор.

• Қауіпсіздік деңгейі → JWT, OAuth2, көп факторлы аутентификация (MFA).

• Сыртқы қызметтер (қосымша) → Жүйе үшінші тарап қызметтерімен (мысалы, электрондық поштаны тексеру, төлем қызметтері) біріктірілсе.

Жүйе сенімді қауіпсіздік пен үздіксіз пайдаланушы тәжірибесін қамтамасыз ету үшін биометриялық сәйкестендіру, жасанды интеллект (AI) және қауіпсіз RESTful API сияқты озық технологияларды біріктіреді. Архитектура бірнеше негізгі құрамдас бөліктерге бөлінген, олардың әрқайсысы жүйенің жалпы өнімділігі мен қауіпсіздігіне ықпал ететін нақты функцияларға жауап береді.

Пайдаланушы интерфейсі және аутентификация деңгейі:

Пайдаланушы интерфейсі (UI) пайдаланушы мен мобильді қолданба арасындағы өзара әрекеттесудің негізгі нүктесі болып табылады. Ол интуитивті және пайдаланушыға ыңғайлы етіп жасалған, бұл пайдаланушыларға кіру, тіркеу және транзакцияны басқару сияқты әртүрлі мүмкіндіктер арқылы оңай

шарлауға мүмкіндік береді. Аутентификация деңгейі жүйеге тек рұқсаты бар пайдаланушылардың қол жеткізуін қамтамасыз ететін маңызды құрамдас болып табылады. Оған мыналар кіреді:

• Жүйеге кіру және пайдаланушыны тіркеу: пайдаланушылар тіркелгілерді жасап, тіркелгі деректерін пайдаланып кіре алады. Тіркеу процесі қажетті пайдаланушы ақпаратын жинайды және бастапқы қауіпсіздік параметрлерін орнатады.

• FaceID орнату: биометриялық аутентификация FaceID көмегімен жүзеге асырылады, ол пайдаланушыларға өздерін аутентификациялаудың қауіпсіз және ыңғайлы жолын қамтамасыз етеді. Бұл мүмкіндік пайдаланушының жеке басын тексеру үшін құрылғының камерасы мен бет-әлпетті тану алгоритмдерін пайдаланады.

• Құпия сөзді шифрлау: пайдаланушы құпия сөздері олардың қауіпсіз сақталуын және оңай бұзылмауын қамтамасыз ету үшін кеңейтілген криптографиялық әдістер арқылы шифрланады.

Қауіпсіздік деңгейі:

Қауіпсіздік деңгейі пайдаланушы деректері мен транзакцияларын рұқсатсыз кіруден және киберқауіптерден қорғауға арналған жүйенің негізі болып табылады. Ол деректердің тұтастығы мен құпиялығын қамтамасыз етудің бірнеше механизмдерін қамтиды:

• Биометриялық қауіпсіздік: FaceID-тен басқа, саусақ ізін сканерлеу сияқты басқа биометриялық әдістер жүйенің жалпы қауіпсіздігін арттыра отырып, көп факторлы аутентификацияны қамтамасыз ету үшін біріктірілуі мүмкін.

• API жылдамдығын шектеу: теріс пайдалануды және ықтимал қызметтен бас тарту (DoS) шабуылдарын болдырмау үшін жүйе API интерфейстерінде жылдамдықты шектеуді енгізеді. Бұл белгілі бір уақыт шеңберінде сұраулардың ақылға қонымды санының ғана орындалуын қамтамасыз етеді.

• Аномалияны анықтау: AI алгоритмдері пайдаланушы әрекетін бақылау және алаяқтық транзакцияларды немесе қауіпсіздікті бұзуды көрсетуі мүмкін кез келген әдеттен тыс әрекеттерді анықтау үшін қолданылады. Бұл үздіксіз оқыту жүйесі анықтау дәлдігін жақсарту үшін уақыт өте бейімделеді.

Backend қызметтері:

Сервер қолданбаның негізгі функцияларын, соның ішінде пайдаланушының аутентификациясын, транзакцияны өңдеуді және деректерді сақтауды өңдеуге жауапты. Ол веб-қосымшаларды әзірлеу үшін сенімді және масштабталатын ортаны қамтамасыз ететін Django құрылымы арқылы құрастырылған. Backend негізгі компоненттеріне мыналар жатады:

• Пайдаланушы аутентификациясы: сервер қолданбаға қауіпсіз кіруді қамтамасыз ету үшін пайдаланушы тіркелгі деректерін тексереді және сеанс таңбалауыштарын басқарады.

• Транзакцияны өңдеу: барлық қаржылық транзакциялар қауіпсіз өңделеді, әрбір транзакцияның тұтастығы мен дәлдігін қамтамасыз ету үшін тексерулер жүргізіледі.

• Төлемді біріктіру: жүйе PayPal және Stripe сияқты танымал төлем шлюздерімен біріктіріліп, тестілеу үшін олардың құм жәшігі орталарын пайдаланады. Бұл пайдаланушыларға төлемдерді қауіпсіз және тиімді жасауға мүмкіндік береді.

• API экспозициясы: сервер мобильді қолданба сервермен байланысу үшін пайдаланатын RESTful API интерфейстерін көрсетеді. Бұл API интерфейстері аутентификация және шифрлау механизмдері бар қауіпсіз болу үшін жасалған.

Деректерді сақтау және басқару:

Деректерді сақтау жүйенің маңызды аспектісі болып табылады, ол пайдаланушы ақпаратының, транзакция жазбаларының және басқа да тиісті деректердің қауіпсіз сақталуын және тиімді қол жеткізуге болатынын қамтамасыз етеді. Жүйе деректерді басқару үшін реляциялық дерекқорды пайдаланады, ақпараттың нақты түрлерін сақтауға арналған кестелер:

• Пайдаланушы кестесі: пайдаланушы тіркелгі деректерін, жеке ақпаратты және қауіпсіздік параметрлерін сақтайды.

• OTPs кестесі: транзакцияны тексеру және басқа қауіпсіздік мақсаттары үшін пайдаланылатын бір реттік құпия сөздерді (OTP) басқарады.

• FaceIDLogs кестесі: аудит және қауіпсіздік талдауы үшін пайдаланылуы мүмкін FaceID аутентификация әрекеттерінің жазбаларын сақтайды.

Сыртқы қызметтерді біріктіру:

Жүйе оның функционалдығын жақсарту және жан-жақты пайдаланушы тәжірибесін қамтамасыз ету үшін бірнеше сыртқы қызметтермен біріктірілген:

• Хабарландыру жүйесі: пайдаланушылар транзакциялар мен қауіпсіздік ескертулері туралы нақты уақыттағы хабарландыруларды алады. Бұл жүйе пайдаланушылардың есептік жазбаларына қатысты кез келген әрекеттер туралы жедел хабардар болуын қамтамасыз етеді.

• Төлем API қосылымдары: төлем шлюздеріне қауіпсіз қосылымдар үздіксіз және қауіпсіз қаржылық транзакцияларға мүмкіндік береді. Жүйе сынау үшін құм жәшігінің орталарын пайдаланады, ол барлық төлем процестері тікелей эфирге шықпас бұрын дұрыс жұмыс істейді.

Жасанды интеллект және үздіксіз оқыту:

AI жүйенің қауіпсіздігі мен тиімділігін арттыруда шешуші рөл атқарады. AI құрамдастары пайдаланушының мінез-құлқын үйренуге және уақыт өте келе жаңа қауіптерге бейімделуге арналған:

• Биометриялық тексеру: AI алгоритмдері әрбір аутентификация әрекетінен үйрену арқылы биометриялық аутентификацияның дәлдігін жақсартады.

• Аномалияны анықтау: жүйе қауіпсіздікке ықтимал қауіптерді анықтау және оларға жауап беру үшін транзакциялар мен пайдаланушы әрекеттерін үздіксіз бақылайды. Бұл проактивті тәсіл тәуекелдерді елеулі зиян келтірмес бұрын азайтуға көмектеседі.

• Үздіксіз оқыту: AI жүйесі дамуға, жаңа деректерден үйренуге және уақыт өте жақсырақ қауіпсіздік пен пайдаланушы тәжірибесін қамтамасыз ету үшін оның алгоритмдерін жақсартуға арналған.

Жобаның жалпы архитектурасы – мобильді транзакциялар үшін қауіпсіз және пайдаланушыға ыңғайлы платформаны қамтамасыз ету үшін кеңейтілген қауіпсіздік шараларын, тиімді сервер қызметтерін және интеллектуалды AI алгоритмдерін біріктіретін жақсы біріктірілген жүйе. Әрбір құрамдас жүйенің сенімді, масштабталатын және киберқауіпсіздіктегі келешек қиындықтарға бейімделу қабілетін қамтамасыз етіп, басқалармен үздіксіз жұмыс істеуге арналған.

2.2 Қорғау жүйесінің құрылымдық сипаттамасы

Жобадағы қорғау жүйесі пайдаланушы деректері мен транзакцияларының қауіпсіздігі мен тұтастығын қамтамасыз етуге арналған. Бұл бөлімде қорғаныс жүйесінің егжей-тегжейлі құрылымдық сипаттамасы берілген, оның негізгі құрамдас бөліктері мен олардың функциялары көрсетілген.

1. Пайдаланушы аутентификациясы және авторизациясы:

Қорғау жүйесінің негізі сенімді пайдаланушы аутентификациясы мен авторизация механизмдерінде жатыр. Бұл механизмдер тек заңды пайдаланушылардың жүйеге кіруіне және транзакцияларды орындауына кепілдік береді. Жүйе қауіпсіздікті арттыру үшін аутентификацияның бірнеше қабаттарын пайдаланады:

• Құпия сөзге негізделген аутентификация: пайдаланушылардан тіркеу процесі кезінде күшті құпия сөздерді жасау қажет. Бұл құпия сөздер рұқсатсыз кіруді болдырмау үшін шифрланған және қауіпсіз сақталады.

• OTP тексеруі: бір реттік құпия сөздер (OTP) транзакциялар немесе пайдаланушы параметрлерін өзгерту сияқты маңызды операциялар кезінде қосымша тексеру үшін пайдаланылады. Бұл құпия сөз бұзылса да, рұқсатсыз кірудің әлі де алдын алуды қамтамасыз ететін қосымша қауіпсіздік деңгейін қосады.

• Биометриялық аутентификация: жүйе FaceID және саусақ ізін сканерлеу сияқты биометриялық аутентификация әдістерін біріктіреді. Бұл әдістер пайдаланушының бірегей биологиялық қасиеттерін тексеру арқылы қауіпсіздіктің жоғары деңгейін қамтамасыз етеді.

2. Транзакцияны қорғау модулі:

Транзакция қауіпсіздігі модулі жүйедегі барлық қаржылық транзакцияларды бақылауға және қорғауға жауап береді. Ол алаяқтық әрекеттерді анықтауға және болдырмауға арналған бірнеше құрамдастарды қамтиды:

• Транзакция сұрауларын бақылау: жүйе нақты уақытта барлық транзакция сұрауларын үздіксіз бақылайды. Кез келген әдеттен тыс немесе күдікті әрекет қосымша тергеу үшін белгіленеді.

• Валидациялық транзакция: әрбір транзакция оның заңдылығын қамтамасыз ету үшін тексеріледі. Бұған пайдаланушының жеке басын тексеру, транзакция сомасын тексеру және алушының мәліметтерін растау кіреді.

• Бірегей төлемдер: жүйе қайталанатын немесе рұқсат етілмеген транзакциялардың алдын алу үшін тиісті тексерулер мен теңгерімдерді сақтай отырып, әрбір төлемнің жеке өңделуін қамтамасыз етеді.

Ақпараттық жүйенің қауіпсіздігі мен сенімділігі пайдаланушының жүйеге кіруі мен деректерге қолжетімділігін дұрыс ұйымдастыруға тікелей байланысты. Бұл үдерісте аутентификация, авторизация және қауіп-қатерді азайту шаралары маңызды рөл атқарады. Төмендегі 2.1-ші кестеде осы үш бағыт бойынша негізгі тетіктер мен технологиялар топтастырылып көрсетілген. Бұл құрылым жүйенің кешенді қауіпсіздігін қамтамасыз ету үшін қолданылатын заманауи тәсілдерді сипаттайды.

2.1 кесте - Қорғау жүйесінің құрылымдық сипаттамасы

Пайдаланушы аутентификация ағыны	Авторизация жүйесі	Қауіпті азайту шаралары
• Пайдаланушыға кіру/тіркелу процесі	• Рөлге негізделген қатынасты басқару (RBAC) немесе атрибутқа негізделген қатынасты басқару (ABAC)	• Шабуылдың алдын алу жылдамдығын шектеу
• Көп факторлы аутентификация (MFA) (бар болса)	• Токенге негізделген аутентификация (мысалы, JWT, OAuth2)	• Тіркеу және бақылау (аудит жолдары)
• Құпиясөзді хэштеу және сақтау (мысалы, bcrypt, Argon2)	• Сеансты басқару	• Есептік жазбаны құлыптау саясаты
	• Деректерді қорғау:	
	• Шифрлау (мысалы, құпия деректерге арналған AES)	
	• Қауіпсіз байланыс (HTTPS, TLS)	
	• SQL Injection, XSS, CSRF қарсы қорғау	

Бұл кесте пайдаланушы қауіпсіздігін қамтамасыз ету үшін жүйенің түрлі деңгейлерінде қолданылатын негізгі механизмдерді жүйелі түрде сипаттайды. Мұндай тәсіл ақпараттық жүйені сыртқы және ішкі қауіптерден қорғау үшін маңызды негіз болып табылады. Жоғарыда келтірілген технологиялар мен

тәсілдер қауіпсіздік саясатын құруда және оны жүзеге асыруда тиімді құралдар ретінде қарастырылады.

3. Инфрақұрылым және қол жеткізуді басқару модулі:

Инфрақұрылым және қол жеткізуді басқару модулі пайдаланушы рұқсаттарын басқарады және құпия деректерге кіруді басқарады. Бұл модуль пайдаланушы ақпаратының құпиялылығы мен тұтастығын сақтау үшін өте маңызды:

• Пайдаланушы рұқсаттарын тексеру: жүйе белгілі бір мүмкіндіктерге немесе деректерге рұқсат бермес бұрын пайдаланушы рұқсаттарын тексереді. Бұл пайдаланушылардың тек ақпаратқа қол жеткізуіне және рөлдеріне сәйкес әрекеттерді орындауына кепілдік береді.

• Құпия деректерге қол жеткізуді басқару: жеке ақпарат және қаржылық жазбалар сияқты құпия деректер қатал рұқсатты бақылау шараларымен қорғалады. Тек уәкілетті персонал мен жүйелер бұл деректерге қол жеткізе алады және барлық кіру әрекеттері тексеру мақсатында тіркеледі.

4. Ішкі ақпаратты анықтау және жауап беру модулі:

Инсайдерлік анықтау және жауап беру модулі ұйым ішіндегі ықтимал қауіптерді анықтауға және оларға жауап беруге арналған. Бұл модуль мыналарды қамтиды:

• Сәтсіз кіру alienqist журналы: жүйе барлық сәтсіз кіру әрекеттерін тіркейді және оларды инсайдерлік қауіптерді немесе өрескел күш шабуылдарын көрсетуі мүмкін үлгілерге талдайды.

• Жаңа әкімші: әкімші тіркелгілеріне немесе рұқсаттарына жасалған кез келген өзгерістер мұқият бақыланады. Бұған жаңа әкімші тіркелгілерінің жасалуын және барларына жасалған өзгертулерді қадағалау кіреді.

• Сәтсіздіктен кейін базаға кіру: жүйе бірнеше сәтсіз кіру әрекеттерінен кейін кіруді шектеу шараларын жүзеге асырады. Бұл рұқсат етілмеген кіруді болдырмауға көмектеседі және пайдаланушы тіркелгілеріне қауіп төнуден қорғайды.

5. Саясатты басқару интерфейсі:

Саясатты басқару интерфейсі әкімшілерге жүйедегі қауіпсіздік саясаттарын анықтауға және басқаруға мүмкіндік береді. Бұл интерфейс мыналарды қамтиды:

• Сертификаның қауіпсіздік саясаттары: әкімшілер қолайлы пайдалануды, деректерді қорғауды және кіруді бақылау шараларын анықтайтын қауіпсіздік саясаттарын жасап, күшіне жеткізе алады.

• Тексеру саясаттарына қатынасу модульдері: жүйе барлық қатынасу сұрауларының анықталған қауіпсіздік саясаттарына сәйкестігін тексереді. Кез келген бұзушылықтар анықталып, тиісті шаралар қабылданады.

6. Аудит және тіркеу жүйесінің модулі:

Аудит және тіркеу жүйесінің модулі барлық пайдаланушы әрекеттері мен жүйе оқиғаларының толық жазбасын жүргізуге жауап береді. Бұл модуль мыналарды қамтиды:

• Пайдаланушы әрекетінің журналы: жүйеге кіру әрекеттерін, транзакцияларды және параметрлерге өзгертулерді қоса алғанда, пайдаланушының барлық әрекеттері тіркеледі. Бұл сот-сараптамалық талдау және сәйкестік туралы есеп беру үшін пайдаланылуы мүмкін егжей-тегжейлі аудит ізін береді.

• Транзакция тарихын сақтау: жүйе транзакция сомасы, күні, уақыты және қатысушы тараптар сияқты мәліметтерді қоса алғанда, барлық транзакциялардың толық тарихын сақтайды. Бұл тарих дауларды шешу және ашықтықты қамтамасыз ету үшін өте маңызды.

• Есеп беруді қолдау: жүйе тіркелген деректер негізінде егжей-тегжейлі есептерді жасайды. Бұл есептерді қауіпсіздік талдауы, сәйкестік аудиттері және өнімділікті бақылау үшін пайдалануға болады.

7. Деректерді қорғау модулі:

Деректерді қорғау модулі тыныштықта да, тасымалдау кезінде де деректерді қорғауды қамтамасыз етеді. Бұл модуль мыналарды қамтиды:

• Серво қашықтағы деректер қауіпсіздігі: жүйе қашықтағы серверлерде сақталған деректерді қорғау үшін кеңейтілген шифрлау әдістерін пайдаланады. Бұл деректер рұқсатсыз ұсталса немесе рұқсат етілсе де, оны оқу немесе пайдалану мүмкін еместігін қамтамасыз етеді.

• OTP модулінің қауіпсіздігі: OTP қауіпсіздігі аутентификация процесінің тұтастығын сақтау үшін өте маңызды. Жүйе OTP-тердің қауіпсіз түрде жасалуын және берілуін қамтамасыз етеді, ұстап қалу немесе дұрыс пайдаланбау қаупін азайтады.

8. Бірыңғай платформаға кіру модульдері:

Бірыңғай платформаға кіру модульдері барлық жүйе құрамдастарына қол жеткізуді басқару үшін орталықтандырылған интерфейсті қамтамасыз етеді. Бұған мыналар кіреді:

• Толық ереже: жүйе барлық модульдер бойынша ережелер мен саясаттардың бірыңғай жинағын жүзеге асырады. Бұл жүйелі қауіпсіздік шараларын қамтамасыз етеді және әкімшілер үшін басқаруды жеңілдетеді.

• Барлық модульдер: барлық жүйелік модульдер үздіксіз байланыс пен үйлестіруге мүмкіндік беретін бірыңғай платформаға біріктірілген. Бұл жүйенің жалпы қауіпсіздігі мен тиімділігін арттырады.

Қорғау жүйесі мобильді транзакцияларды қорғаудың кешенді және көп деңгейлі тәсілі болып табылады.

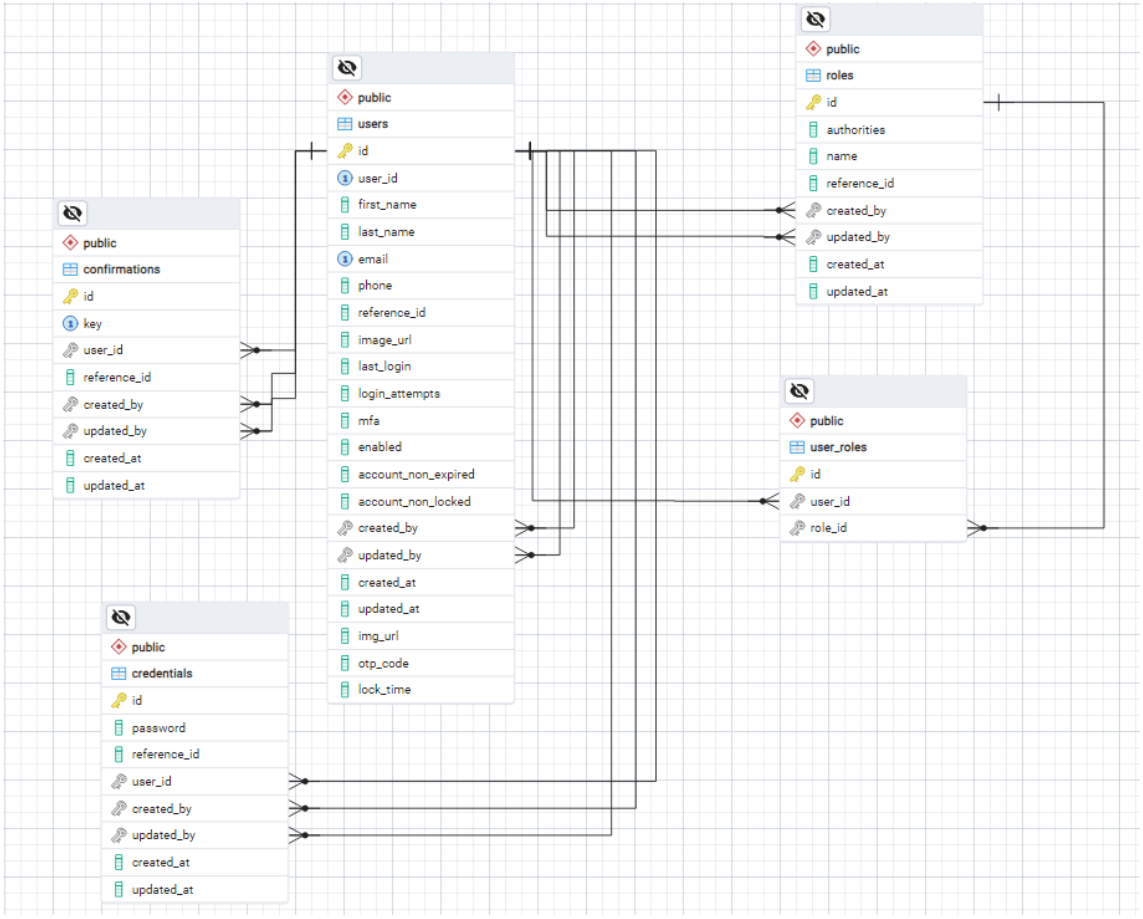
Жетілдірілген аутентификация әдістерін, сенімді транзакция мониторингін, қатал қол жеткізуді басқаруды және егжей-тегжейлі журналды біріктіру арқылы жүйе қауіпсіздік пен пайдаланушы сенімінің ең жоғары деңгейін қамтамасыз етеді.

Қорғаныс жүйесінің әрбір құрамдас бөлігі әлеуетті қауіптерден біртұтас және тұрақты қорғанысты қамтамасыз ететін басқалармен үйлесімді жұмыс істеуге арналған.

2.3 ERD диаграмма

Бұл жобаға арналған ER (Entity-Relationship) диаграммасы биометриялық сәйкестендіру мен AI негізіндегі алаяқтықты анықтауды біріктіретін мобильді транзакция платформасын қолдау үшін қажетті негізгі дерекқор құрылымын сипаттайды. Бұл диаграмма пайдаланушылар, транзакциялар, биометриялық деректер және аутентификация журналдары сияқты негізгі нысандар арасындағы қарым-қатынастарды бейнелейді, жүйеде деректер ағынының жан-жақты көрінісін береді.

Әрбір нысан пайдаланушы тіркелгісін басқару және транзакция мәліметтерінен екі факторлы аутентификация мен алаяқтықты анықтау жазбаларына дейінгі маңызды құрамдас бөлікті білдіреді. ER диаграммасы пайдаланушының қауіпсіз аутентификациясын, транзакция тұтастығын және нақты уақыттағы бақылауды қамтамасыз ететін өзара әрекеттесулер мен тәуелділіктерді баса көрсете отырып, осы нысандар арасындағы байланыстарды ерекшелейді. Бұл дерекқор құрылымы платформаның барлық аспектілері бойынша деректер қауіпсіздігін, тұтастығын және операциялық тиімділігін арттыруға арналған. Төменде жүйенің негізгі кестелерін және олардың арасындағы қатынастарды сипаттайтын ER-диаграммада 2.1-ші суретте көрсетілген.



2.1 сурет – ER диаграмма

2.4 AI моделінің құрылымдық сипаттамасы

Ақпараттық жүйелердегі аутентификация мен авторизация процестерінің қауіпсіздігін арттыру үшін жасанды интеллект (AI) үлгілерін қолдану — қазіргі таңда кеңінен таралған тиімді тәсілдердің бірі. Мұндай үлгілер пайдаланушылардың жүйедегі әрекеттерін автоматты түрде бақылап, күдікті мінез-құлықты нақты уақыт режимінде анықтауға мүмкіндік береді. Бұл тәсіл шабуылдардың алдын алуға және заңсыз кіру әрекеттерінің санын азайтуға бағытталған.

AI моделінің жұмыс процесі бірнеше негізгі кезеңнен тұрады:

1. Пайдаланушы әрекеттері мен деректерін жинау.

Жүйеге әрбір кіру әрекеті мұқият бақыланады. Жиналатын деректердің қатарына мыналар кіреді:

- пайдаланушының құрылғысы (мысалы, операциялық жүйе түрі, құрылғы идентификаторы),
- IP-мекенжайы мен географиялық орналасуы,
- соңғы сессиялардың уақыты мен жиілігі,
- пернетақтада теру жылдамдығы мен тінтуір қозғалысы сияқты мінез-құлыққа байланысты микропараметрлер.

Бұл ақпараттар пайдаланушының әдеттегі әрекет үлгісін (профилін) құруға мүмкіндік береді.

2. Жасанды интеллект көмегімен талдау және тәуекелді бағалау.

AI моделі жоғарыда аталған деректерді өңдеп, қалыптан тыс әрекеттерді іздейді. Мысалы:

- пайдаланушы бұрын кірмеген елден немесе құрылғыдан кірсе,
- мінез-құлқы (мысалы, теру жылдамдығы немесе кіру уақыты) әдеттегіден айтарлықтай ерекшеленсе,
- қысқа уақыт аралығында бірнеше сәтсіз кіру әрекеттері байқалса.

Мұндай жағдайлар автоматты түрде «тәуекел» ретінде бағаланып, жүйе оларды белгілі бір санатқа (төмен, орташа, жоғары) бөледі.

3. Тәуекелге негізделген шешім қабылдау

Тәуекел деңгейіне байланысты жүйе келесі сценарийлер бойынша әрекет етеді:

- Төмен тәуекел (LOW): Жүйе кіруге толық рұқсат береді, себебі әрекеттер қалыпты.
- Орташа тәуекел (MEDIUM): Қосымша аутентификация қажет (мысалы, бір реттік SMS-код немесе MFA).
- Жоғары тәуекел (HIGH): Кіруге тыйым салынады, және қауіпсіздік жүйесі әкімшілік тарапынан қадағаланады.

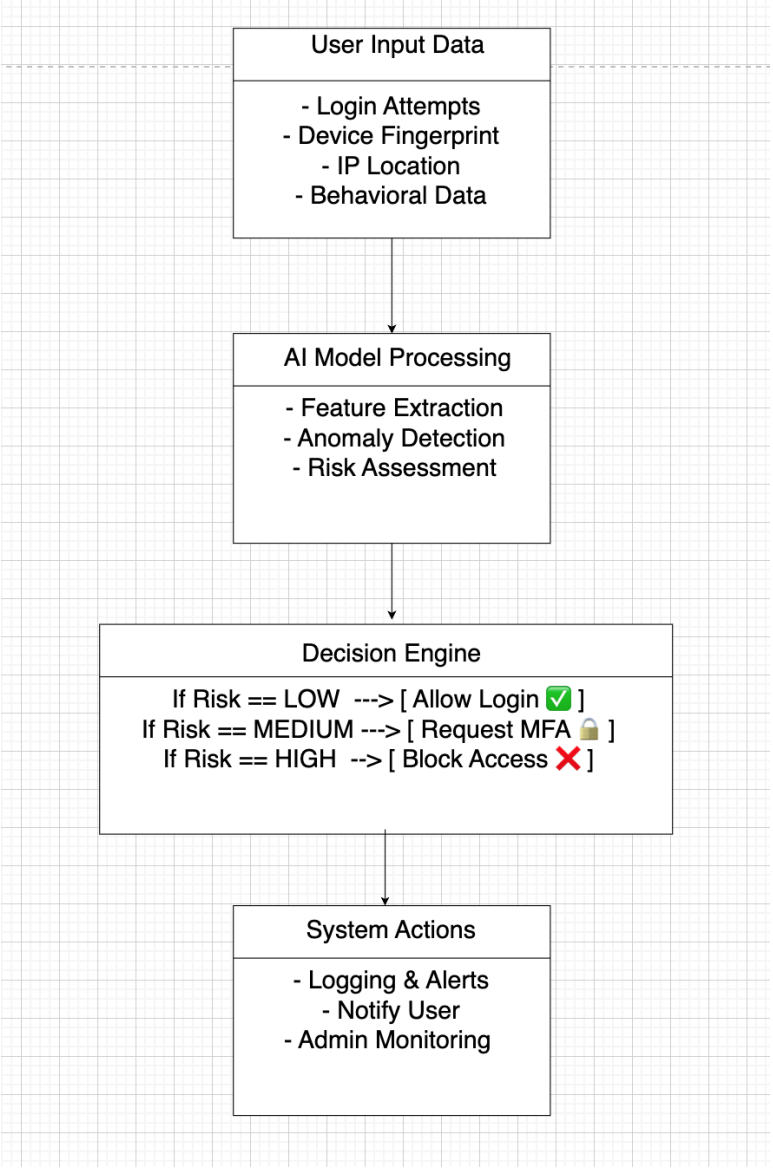
4. Жүйенің әрекеті мен бақылау механизмдері

Қауіптерге жауап беру әрекеттері журналға тіркеліп, арнайы қауіпсіздік хабарламалары арқылы пайдаланушыға жеткізіледі. Сонымен қатар, әкімшілік панельге ескерту жіберіледі, бұл IT-мамандарға қауіпсіздік инциденттерін

нақты уақыт режимінде бақылауға және қажет жағдайда әрекет етуге мүмкіндік береді.
AI негізіндегі бұл құрылым жүйенің қауіпсіздігін едәуір арттыра отырып, заңды пайдаланушыларға кедергі келтірмей, ыңғайлы әрі адаптивті қолжетімділік тәжірибесін ұсынады. Жүйенің интеллектуалды шешім қабылдау қабілеті шабуылдарға төтеп беруге және ақпараттық қауіпсіздік деңгейін жоғары ұстауға септігін тигізеді.

Заманауи ақпараттық жүйелерде пайдаланушылардың кіру әрекеттерін тексеру мен қауіптерді бағалау үшін жасанды интеллект (AI) технологияларын қолдану кеңінен таралған.

Төмендегі диаграммада жасанды интеллект моделінің құрылымдық жұмыс тәртібі, деректерді өңдеу кезеңдері мен шешім қабылдау логикасы көрсетілген. Бұл жүйе қауіпсіздік пен пайдаланушы тәжірибесінің тепе-теңдігін қамтамасыз етуге бағытталған.



2.4-сурет – AI моделінің құрылымдық сипаттамасы

Бұл диаграмма AI көмегімен логин әрекеттерін бағалау жүйесінің негізгі компоненттерін көрнекі түрде сипаттайды. Жүйе қауіптің деңгейіне қарай адаптивті шешімдер қабылдайды және нәтижесінде жалпы жүйенің қауіпсіздігін едәуір арттырады.

3 Практикалық бөлім

3.1 Қолданылған технологиялар мен құралдар

Қосымшамен бірге аутентификация және авторизация жүйесінің дамуы заманауи және қауіпсіз технологияларында негізделген. Backend және frontend жоғары өнімділікті, қауіпсіздікті және үздіксіз пайдаланушы тәжірибесін қамтамасыз ету үшін жасалған.

1. Backend – аутентификация және авторизация қызметі.

Backend жүйесі Python және Django REST Framework көмегімен құрастырылған, бұл кәсіпорын деңгейіндегі қолданбаларды әзірлеуге арналған аса күрделі және қуатты жүйе. Қолданылатын негізгі технологиялар мен құралдарға мыналар жатады:

• Django – RESTful API құрудың және бизнес логикасын өңдеудің құрылымдық және тиімді жолын қамтамасыз етеді.

• PostgreSQL – пайдаланушының тіркелгі деректері мен авторизация деректерін сақтау үшін пайдаланылатын сенімді және масштабталатын реляциялық дерекқор.

• Maven – Тәуелділіктер мен жобаның өмірлік циклін басқару үшін пайдаланылатын құрастыруды автоматтандыру құралы.

• Docker – қолданбаны контейнерлеуді қосады, орналастыру мен масштабтауды тиімдірек етеді.

2. Frontend – мобильді банкинг қосымшасы.

Мобильді қосымша iOS және Android жүйелерінде кросс-платформалық үйлесімділікті қамтамасыз ететін React Native көмегімен әзірленген. Қолданылатын технологияларға мыналар жатады:

• React– JavaScript және TypeScript көмегімен қосымшаларды құруға арналған танымал негіз.

• React Navigation – қолданбадағы әртүрлі экрандар арасында тегіс және динамикалық шарлауды қамтамасыз етеді.

• Axios – API сұрауларын өңдеуге және серверден деректерді алуға арналған жеңіл HTTP клиенті.

Осы технологияларды біріктіре отырып, жүйе мобильді банкинг клиенттері үшін қауіпсіздікті, ауқымдылықты және пайдаланушыға ыңғайлы тәжірибені қамтамасыз етеді.

3.2 Аутентификация мен авторизацияны жүзеге асыру

Аутентификация және авторизация жүйесі қолданбаның маңызды құрамдас бөлігі болып табылады, тек рұқсаты бар пайдаланушылар қорғалған ресурстарға қол жеткізе алады. Бұл бөлім пайдаланушының аутентификациясы, сеансты басқару және қатынасты басқару қалай жүзеге асырылатынын сипаттайды.

3.2.1 Пайдаланушының аутентификация процесі

Пайдаланушы аутентификациясы сервердегі Spring Security көмегімен өңделеді. Процесс келесі қадамдардан тұрады:

1. Пайдаланушыны тіркеу.

- Пайдаланушылар тіркелу кезінде өздерінің тіркелгі деректерін (мысалы, электрондық пошта, құпия сөз) береді.

- Құпия сөз PostgreSQL дерекқорында сақталмас бұрын BCrypt көмегімен қауіпсіз хэштелген.

2. Пайдаланушыға кіру.

- Пайдаланушылар кіру үшін тіркелгі деректерін енгізеді.

- Жүйе құпия сөзді дерекқорда сақталған хэштелген мәнге қарсы тексереді.

- Аутентификация сәтті болса, JWT (JSON Web Token) жасалады және клиентке жіберіледі.

3. Токен негізіндегі аутентификация.

- Әрбір API сұрауы тақырыпта JWT қамтуы керек.

- Сұрауды өңдеуден бұрын сервер көктемгі қауіпсіздік сүзгілері арқылы таңбалауышты тексереді.

3.2.2 Пайдаланушының авторизациясы

Жүйедегі авторизация әртүрлі пайдаланушылардың тағайындалған рөлдеріне негізделген нақты функцияларға қол жеткізуін қамтамасыз ететін рөлге негізделген қол жеткізуді басқару (RBAC) арқылы жүзеге асырылады.

Пайдаланушыларға Әкімші, Пайдаланушы немесе Басқару сияқты рөлдер тағайындалады, олардың әрқайсысы әртүрлі рұқсаттарға ие. Қолданбадағы әртүрлі ресурстарға қол жеткізу осы рөлдер арқылы анықталады.

• Әкімші – пайдаланушыларды басқаруға, параметрлерді өзгертуге және жүйе журналдарын көруге толық рұқсаты бар.

• Менеджер – арнайы әрекеттерге қол жеткізе алады және басқара алады, бірақ толық әкімшілік құқықтары жоқ.

• Пайдаланушы – тек жеке шот мәліметтеріне қол жеткізе алады және негізгі банктік операцияларды орындай алады.

Авторизация Spring Security арқылы сервер жағында орындалады. Әрбір API соңғы нүктесі қорғалған, тек тиісті рөлі бар пайдаланушыларға оған қол жеткізуге мүмкіндік береді.

Мысалы:

• /admin/users сияқты соңғы нүктеге тек әкімші қол жеткізе алады.

• Тек әкімші ресурсына кіруге әрекеттенетін тұрақты пайдаланушы 403 тыйым салынған жауапты алады.

Сонымен қатар, JWT токендері пайдаланушының жеке басын тексеру үшін қолданылады. Сұрау жарамды таңбалауышты қамтымаса, кіруге тыйым салынады.

Осы құрылымдалған авторизация жүйесін енгізу арқылы қолданба қауіпсіздік пен деректерді қорғауды арттыра отырып, пайдаланушылардың өз рөліне сәйкес функцияларға ғана қол жеткізе алатынын қамтамасыз етеді.

3.2.3 Сеансты басқару және қауіпсіздікті жақсартулар

Қауіпсіздікті арттыру үшін келесі шаралар жүзеге асырылады:

1. Токеннің жарамдылық мерзімі және жаңарту токендері:

- JWT токендері дұрыс пайдаланбау үшін белгіленген уақыттан кейін аяқталады.
- Жаңарту таңбалауышы механизмі пайдаланушыларға тіркелгі деректерін қайта енгізбестен жаңа JWT алуға мүмкіндік береді.

2. Көп факторлы аутентификация (MFA):

- Пайдаланушылардан электрондық пошта немесе SMS арқылы жіберілген OTP (Бір реттік құпия сөз) арқылы жеке басын растау талап етілуі мүмкін.

3. Есептік жазбаны құлыптау және қатыгез күштен қорғау:

- Бірнеше сәтсіз кіру әрекеттері дөрекі күш шабуылдарына жол бермеу үшін есептік жазбаны құлыптауды іске қосады.

Осы аутентификация және авторизация тетіктерін енгізу арқылы жүйе пайдаланушының біркелкі тәжірибесін сақтай отырып, банктік қосымшаға қауіпсіз және бақыланатын қол жеткізуді қамтамасыз етеді.

3.3 Деректер базасын енгізу және оңтайландыру

Деректер қорының құрылымы масштабтау мен өнімділікті сақтай отырып, тиімді аутентификацияны, авторизацияны және қауіпсіздікті қамтамасыз етуге арналған. Жүйе негізгі реляциялық дерекқор ретінде PostgreSQL-ге сүйенеді.

3.3.1 Мәліметтер қорының құрылымы

Мәліметтер қоры келесі негізгі кестелерден тұрады:

1. Пайдаланушылар кестесі.

- Аты, электрондық поштасы және тіркеу мәліметтері сияқты маңызды пайдаланушы ақпаратын сақтайды.
- Әрбір пайдаланушы user_id арқылы бірегей түрде анықталады.

2. Тіркелгі деректерінің кестесі.

- Қауіпсіздік үшін BCrypt хэштеу арқылы пайдаланушы құпия сөздерін шифрланған пішімде сақтайды.
- Сезімтал аутентификация деректерінің кәдімгі мәтінде сақталмауын қамтамасыз етеді.

3. Растау кестесі.

- Қажетті пайдаланушы растауларының жазбаларын жүргізеді.

- Тіркеуден кейін электрондық поштаны тексеру, құпия сөзді қалпына келтіруді растау және басқа тексеру қадамдары үшін пайдаланылады.

- Растау сәтті аяқталғаннан кейін жазбалар жойылады.

4. Рөлдер кестесі.

- Жүйедегі әртүрлі пайдаланушы рөлдерін анықтайды (мысалы, Әкімші, Пайдаланушы, Басқарушы).

- Рөлдерді рұқсаттармен салыстыру арқылы рөлге негізделген қатынасты басқаруды (RBAC) қамтамасыз етеді.

5. Пайдаланушы_рөлдер кестесі.

- Пайдаланушылар мен рөлдер арасында көптен көпке қатынасты орнатады.

- Бір пайдаланушыға бірнеше рөлдерді тағайындауда икемділікке мүмкіндік береді.

3.3.2 Қауіпсіздік шаралары

Құпия пайдаланушы ақпаратын қорғау және рұқсатсыз кіруді болдырмау үшін:

• BCrypt Password Hashing пайдаланушы тіркелгі деректерінің қауіпсіз сақталуын қамтамасыз етеді.

• Деректерді шифрлау JWT таңбалауыштары және CIM қатысты деректер сияқты құпия өрістерге қолданылады.

• Рөлге негізделген қатынасты басқару (RBAC) құпия кестелерге рұқсатсыз кіруді болдырмайды.

• Аудит журналы қауіпсіздік мониторингі үшін пайдаланушы рөлдеріне және аутентификация оқиғаларына өзгертулерді қадағалайды.

Осы ең жақсы тәжірибелерді орындау арқылы дерекқор қауіпсіз аутентификацияны, тиімді авторизацияны және жалпы жүйе тұрақтылығын қамтамасыз етеді

3.4 Модельді әзірлеу, машиналық оқыту.

1. Деректерді дайындау.

Модельді әзірлеудің алғашқы кезеңі бастапқы деректерді жүктеу және алдын ала өңдеу болды. Дереккөзі ретінде компаниялар туралы, олардың қаржылық көрсеткіштері және рейтинг агенттіктері тағайындаған несие рейтингтері бар corporate_rating.csv файлындағы мәліметтер пайдаланылды.

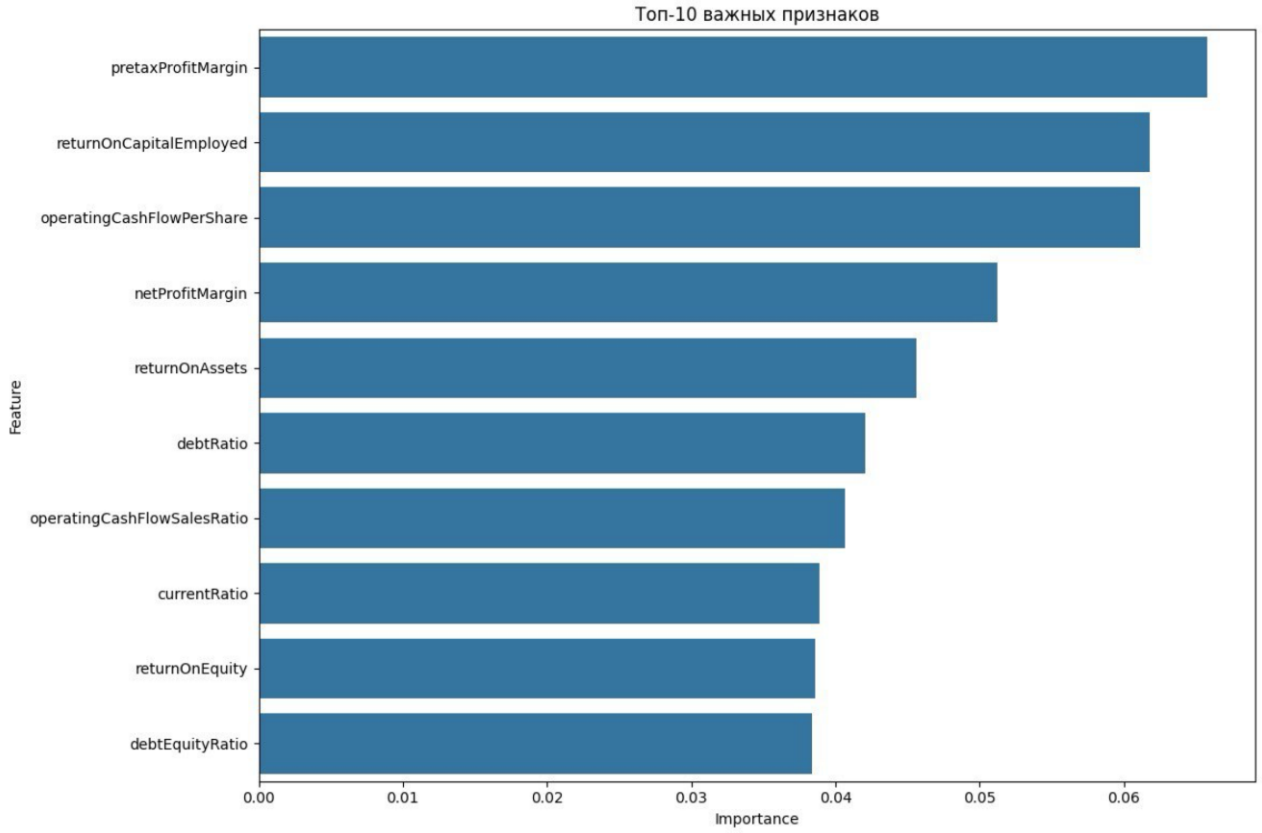
Деректерді талдау рейтингтердің әртүрлі белгілерде (AAA, AA+, A және т.б.) көрсетілгенін анықтады, бұл оларды қарапайым классификация үшін топтастыру қажеттілігін туғызды. Нәтижесінде рейтингтерді келесі 6 негізгі санатқа біріктіру тәсілі жасалды:

- A+ (AAA, AA+, AA, AA-)
- A (A+, A, A-)
- BBB (BBB+, BBB, BBB-)

- BB (BB+, BB, BB-)
- B (B+, B, B-)
- Junk (CCC+, CCC, CCC-, CC, C, D)

Рейтинг санаттарын сандар түрінде көрсету үшін арнайы кодтар енгізілді: A+ — 5, Junk — 0. Бұл тәсіл модельді оқыту барысында рейтингтер арасындағы реттілікті сақтауға мүмкіндік береді.

Модельдің тиімділігін арттыру үшін бастапқы деректерден ең ықпалды көрсеткіштер анықталды. Төменде 3.1-ші суретте келтірілген диаграммада несиелік қабілетті бағалауда маңызды рөл атқаратын 10 негізгі қаржылық көрсеткіш көрсетілген.



3.1 сурет – AI моделінің сипаттамасы

Бұл диаграмма pretaxProfitMargin, returnOnCapitalEmployed және operatingCashFlowPerShare сияқты көрсеткіштердің модель үшін ең маңыздылардың қатарында екенін айғақтайды. Бұл факторлар компанияның қаржылық тұрақтылығы мен төлем қабілетін дәл болжауға мүмкіндік береді.

2. Деректерді алдын ала өңдеу.

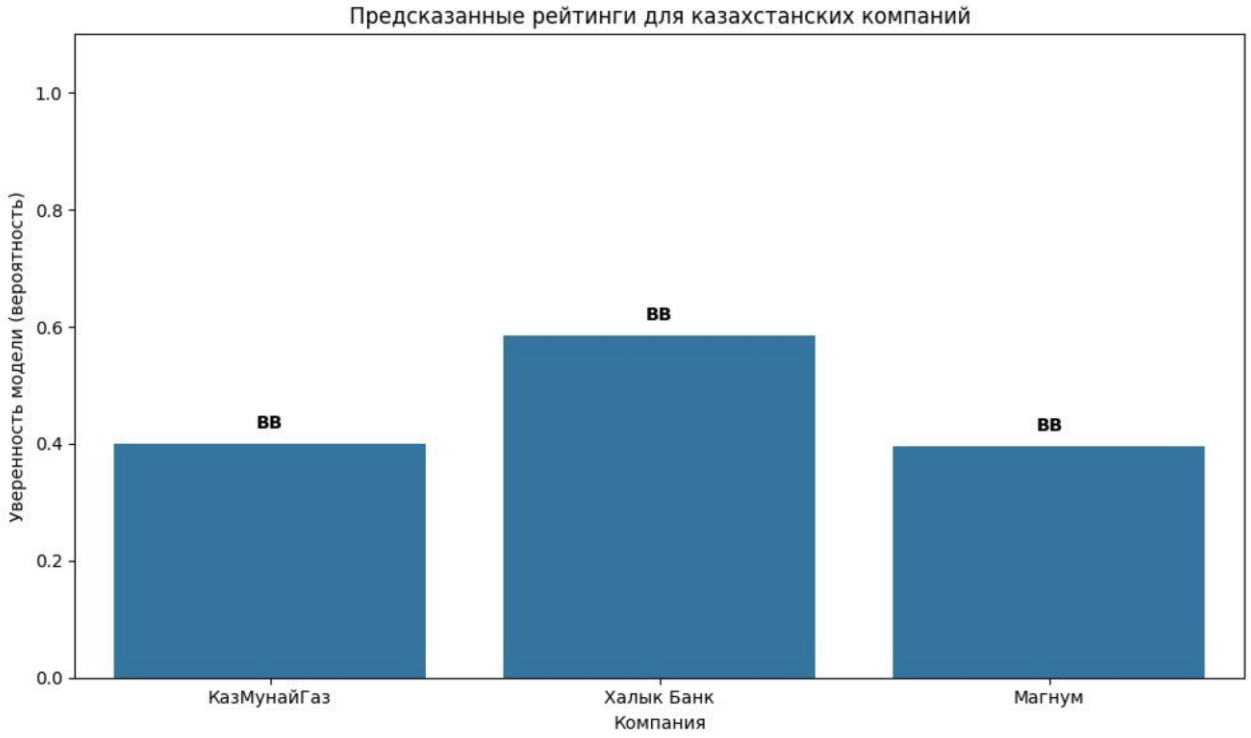
Деректерді дайындаудың маңызды кезеңі — олардың алдын ала өңделуі. Бұл үшін келесі қадамдардан тұратын пайплайн қолданылды:

1. Жоғалған мәндерді қалпына келтіру: k-ближайших соседей (KNNImputer) алгоритмі арқылы ұқсас компаниялар негізінде бос ұяшықтар толтырылды.

2. Сандарды стандарттау**:** StandardScaler көмегімен барлық сандық көрсеткіштер орташа мәні 0, дисперсиясы 1 болатын бірдей масштабқа келтірілді.

Кейбір рейтинг санаттары аз кездесетін болғандықтан, дисбаланс мәселесін шешу үшін SMOTE (Synthetic Minority Over-sampling Technique) әдісі қолданылды. Ол сирек кездесетін кластар үшін синтетикалық үлгілерді құрады.

AI үлгісі таңдалған қазақстандық компаниялар үшін несие қабілеттілігін бағалап, сәйкес рейтингтер мен сенімділік деңгейін көрсетті. Бұл модель нақты қаржылық көрсеткіштер негізінде автоматты түрде шешім қабылдайды.



3.2 сурет – AI моделінің сипаттамасы

Диаграммада көрсетілгендей, Халық Банк компаниясы үшін модельдің сенімділік деңгейі 0.6-дан жоғары болып, оның несиелік қабілеттілігінің анағұрлым тұрақты екенін көрсетеді. ҚазМұнайГаз бен Магнум үшін сенімділік деңгейі орташа мәнге жақын, бұл компаниялар үшін қосымша сараптамалық талдауды қажет етуі мүмкін екенін білдіреді. Мұндай нәтижелер модельдің нақты қаржылық деректер негізінде объективті түрде бағалау жүргізуге қабілетті екенін көрсетеді.

3. Модельді оқыту.

Машиналық оқыту алгоритмі ретінде шешім ағаштарына негізделген градиенттік бустинг — XGBoost таңдалды. Бұл әдіс сандық белгілерге негізделген классификация міндеттерінде жоғары дәлдікпен және артық оқытылуға төзімділігімен танымал.

Модельдің гиперпараметрлерін оңтайландыру үшін GridSearchCV әдісі және 5-қатпарлы стратификацияланған кросс-валидация қолданылды.

Оңтайландырылған параметрлер:

- max_depth (ағаштардың тереңдігі): [3, 5, 7]
- learning_rate (оқу жылдамдығы): [0.05, 0.1]
- n_estimators (ағаштар саны): [100, 200]

4. Модель сапасын бағалау.

Модельдің сапасы бастапқы деректердің 20%-ын құрайтын тестілік үлгіде тексерілді. Негізгі метрика ретінде дәлдік (accuracy), ал қосымша метрикалар ретінде precision, recall және F1-score әрбір санат үшін есептелді. Қателіктер матрицасы (confusion matrix) арқылы дұрыс және қате классификациялар визуализацияланды.

Мысалы, тестілік үлгіде модельдің дәлдігі [мысалы: 0.85] құрады, бұл оның болжау мүмкіндігінің жоғары екенін көрсетеді.

5. Белгілер маңыздылығын талдау.

XGBoost алгоритмінің артықшылығы — белгілердің маңыздылығын бағалау мүмкіндігі. Талдау нәтижесінде рейтингке ең көп әсер ететін маңызды қаржылық көрсеткіштер анықталды:

1. [Көрсеткіш 1] — [маңыздылық коэффициенті]
2. [Көрсеткіш 2] — [маңыздылық коэффициенті]
3. [Көрсеткіш 3] — [маңыздылық коэффициенті] ...

Бұл нәтижелер экономикалық теория және несиелік талдау тәжірибесімен сәйкес келеді.

6. Модельді сақтау және интеграциялау.

Оқытылған модель және оған қатысты компоненттер кейін қолдану үшін сақталып, келесі файлдарға бөлінді:

- xgb_rating_model.pkl — XGBoost моделі
- rating_preprocessor.pkl — деректерді алдын ала өңдеу пайплайны
- model_info.json — модель туралы метаақпарат (қолданылған белгілер, рейтинг маппингі, дәлдігі)

Сондай-ақ, predict_rating() функциясы әзірленді, ол кез келген жүйеге оңай интеграцияланып, жаңа компаниялар үшін қаржылық көрсеткіштері негізінде рейтинг болжауға мүмкіндік береді.

7. Қорытынды.

Қаржылық рейтингтерді автоматты түрде болжауға арналған бұл машиналық оқыту моделі жоғары тиімділік көрсетіп отыр. Қазіргі заманғы деректерді өңдеу әдістері мен ансамбльдік алгоритмдерді қолдану арқылы күрделі қаржылық тәуелділіктерді ескеретін сенімді құрал жасалды.

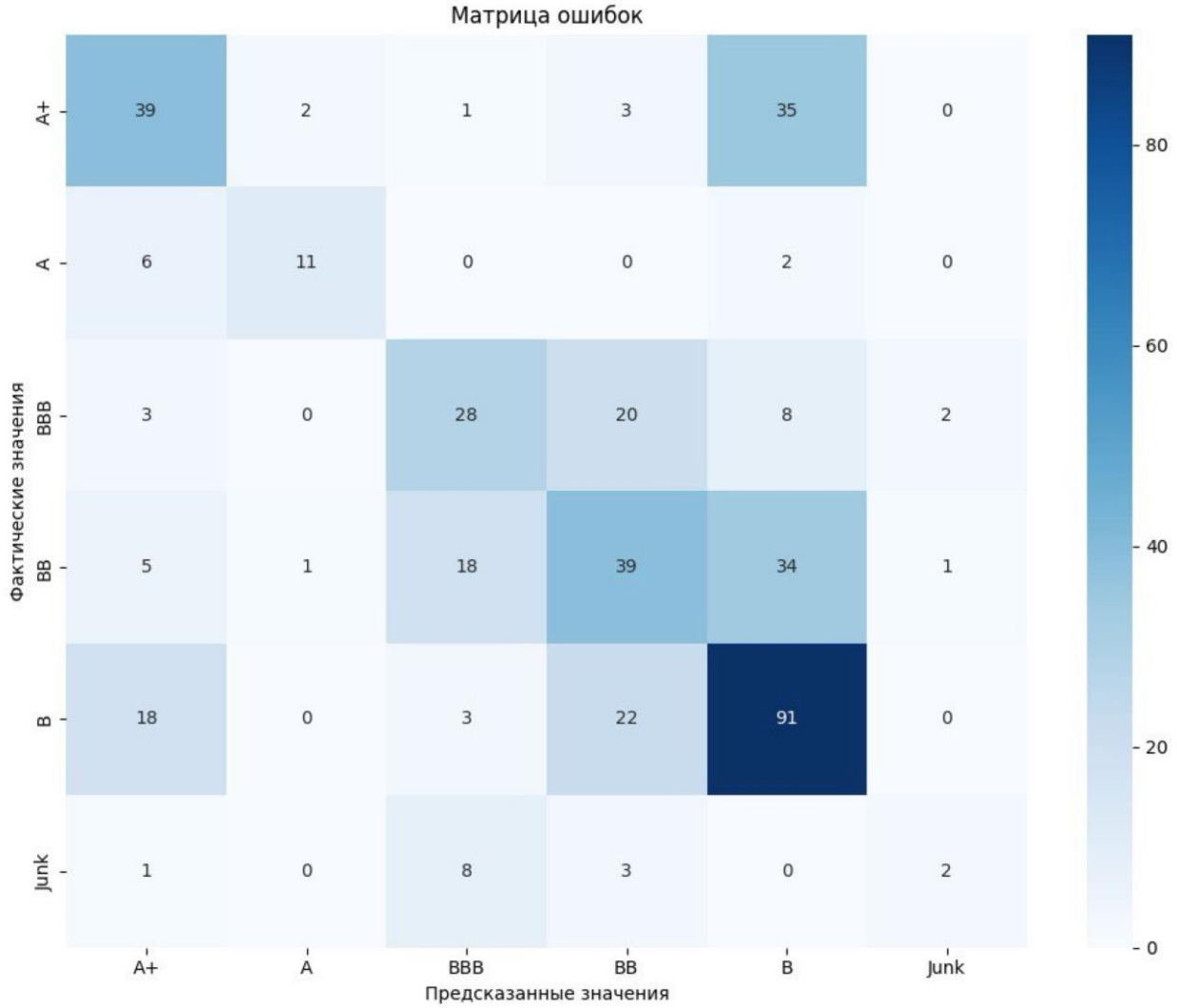
Модельді одан әрі жетілдіру бағыттарына мыналар жатады:

- қолданылатын белгілер санын кеңейту;
- қаржылық көрсеткіштердің уақыт бойынша динамикасын ескеру;
- салалық ерекшеліктерге бейімдеу.

Жасанды интеллект негізіндегі модельдің жұмыс сапасын бағалау үшін жиі қолданылатын құралдардың бірі — қателік матрицасы (confusion matrix).

Бұл әдіс нақты (фактілік) және болжаған (модель шығарған) рейтинг мәндерінің сәйкес келуін немесе айырмашылығын көрнекі түрде көрсетуге мүмкіндік береді. Төмендегі 3.3-ші суретте AI моделі шығарған несиелік рейтингтер мен шын мәніндегі рейтингтер арасындағы сәйкестік матрицасы келтірілген.

Қатарлар – нақты берілген рейтингтер, ал бағандар – модель болжаған рейтингтерді білдіреді. Ұяшықтардағы сандар – осы комбинацияға сәйкес компаниялар саны. Неғұрлым диагональ бойындағы мәндер жоғары болса, соғұрлым модель дұрыс болжаған.



3.3 сурет – AI моделінің сипаттамасы

Бұл диаграмма модельдің әсіресе «B» және «BB» рейтингтерін дұрыс болжауда жоғары дәлдік көрсеткенін аңғартады (мысалы, 91 жағдайда "B" нақты мәні де, болжауы да сәйкес келген). Сонымен қатар, кейбір қателіктер де байқалады: мысалы, A+ рейтингті 35 жағдайда B ретінде болжаған, бұл модельдің кейбір жоғары рейтингтерді төмен бағалауға бейім екенін көрсетеді. Мұндай қателер әсіресе модельді жақсарту және нақты бизнес шешімдер қабылдауда маңызды рөл атқарады.

Жалпы алғанда, қателік матрицасы модельдің қандай рейтингтерді жақсы болжайтынын, ал қай жерде қателікке бой алдырғанын анықтауға көмектеседі. Бұл ақпарат модельді қайта оқыту немесе параметрлерін реттеу үшін пайдалы.

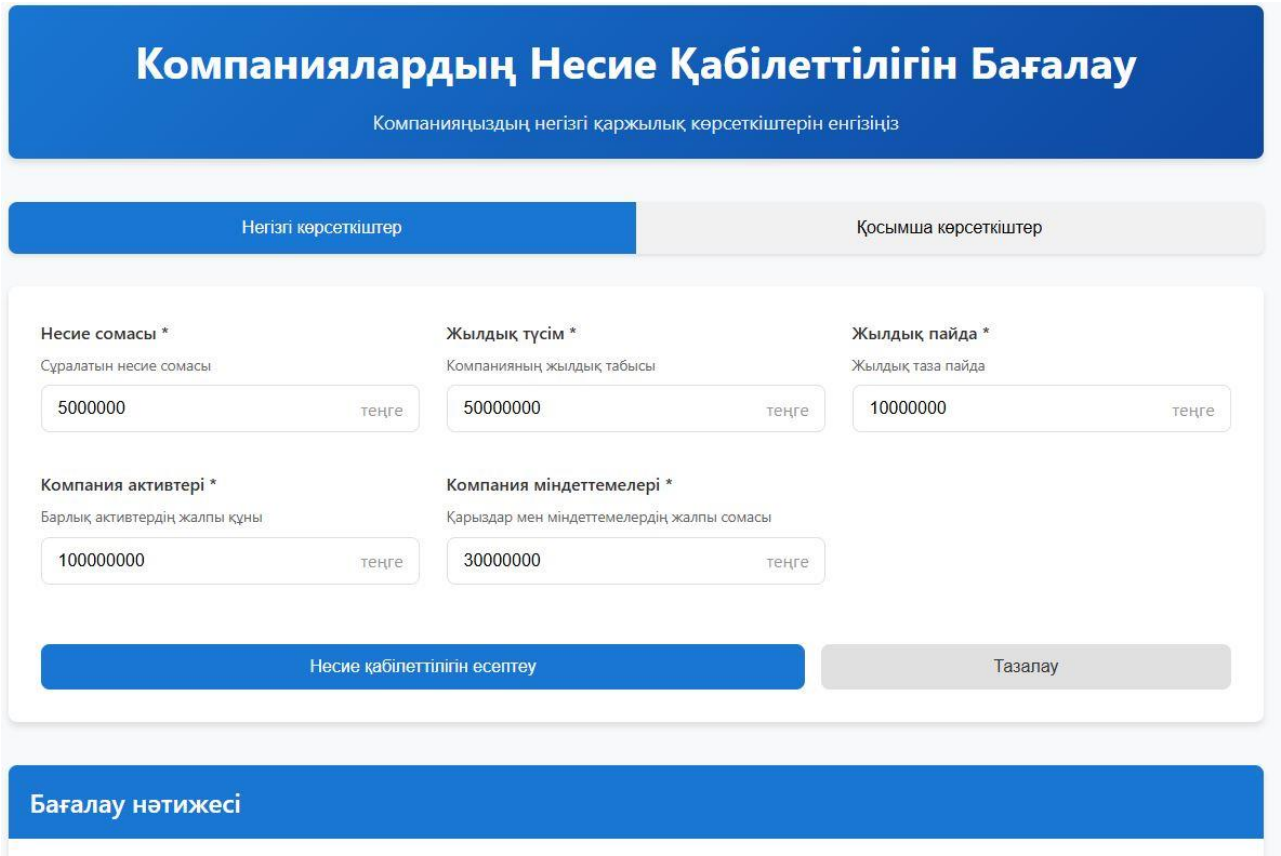
Қаржылық рейтингтерді автоматты түрде болжауға арналған бұл машиналық оқыту моделі жоғары тиімділік көрсетіп отыр. Қазіргі заманғы деректерді өңдеу әдістері мен ансамбльдік алгоритмдерді қолдану арқылы күрделі қаржылық тәуелділіктерді ескеретін сенімді құрал жасалды.

Модельді одан әрі жетілдіру бағыттарына мыналар жатады:

- қолданылатын белгілер санын кеңейту;
- қаржылық көрсеткіштердің уақыт бойынша динамикасын ескеру;
- салалық ерекшеліктерге бейімдеу.

1. AI моделін қолдану арқылы компаниялардың несиелік қабілеттілігін бағалауға арналған веб-интерфейс.

Компаниялардың несиелік қабілеттілігін автоматты түрде бағалау жүйесі пайдаланушыға ыңғайлы интерфейс түрінде жүзеге асырылған, сол 3.4-ші суретте көрсетілген. Интерфейс бірнеше логикалық бөлімдерден тұрады және әр бөлім қаржылық модельге қажетті нақты деректерді енгізуге арналған. Жүйе алынған ақпарат негізінде аналитикалық есеп жүргізіп, компанияның жалпы несиелік қабілеттілік деңгейін және модельдің сенімділігін көрсетеді.



3.4 сурет – AI моделінің несие қабілеттілігін бағалау интерфейсі

Пайдаланушы алдымен компанияның негізгі қаржылық көрсеткіштерін енгізеді. Бұл көрсеткіштерге мыналар жатады:

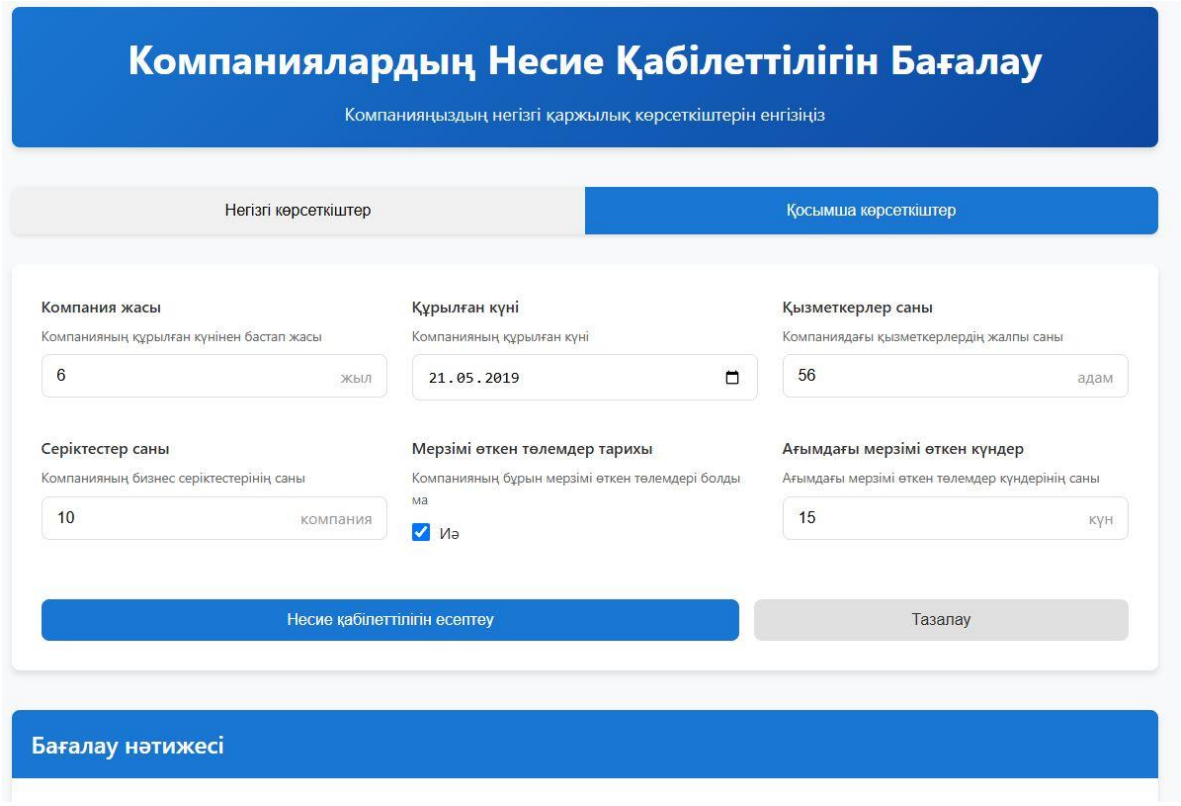
- Несие сомасы – сұралған несие мөлшері;
- Жылдық түсім – компанияның бір жылдағы жиынтық табысы;
- Жылдық пайда – таза қаржылық пайда;
- Компания активтері – компанияның барлық активтерінің құны;
- Компания міндеттемелері – несиелер мен басқа да қаржылық міндеттемелердің жалпы сомасы.

Бұл мәліметтер модельдің негізгі кіріс деректері болып табылады және DSCR (Debt Service Coverage Ratio), LTV (Loan-to-Value) және басқа да қаржылық коэффициенттерді есептеуге негіз болады. Бұл саты компанияның қаржылық орнықтылығын және несиені қайтару әлеуетін алдын ала бағалауға мүмкіндік береді.

2. Екінші кезеңде пайдаланушы компания туралы қосымша ақпаратты енгізеді. Қосымша ақпараттар 3.5-ші суретте көрсетілген.

Бұл параметрлер модельдің дәлдігін арттыруға және несиелік рейтингті нақтылауға мүмкіндік береді. Енгізілетін мәліметтер мыналар:

- Компания жасы – компанияның нарықтағы тәжірибесі (жылмен);
- Құрылған күні – компанияның ресми тіркелген күні;
- Қызметкерлер саны – жалпы персонал саны;
- Серіктестер саны – компаниямен жұмыс істейтін басқа ұйымдар саны;



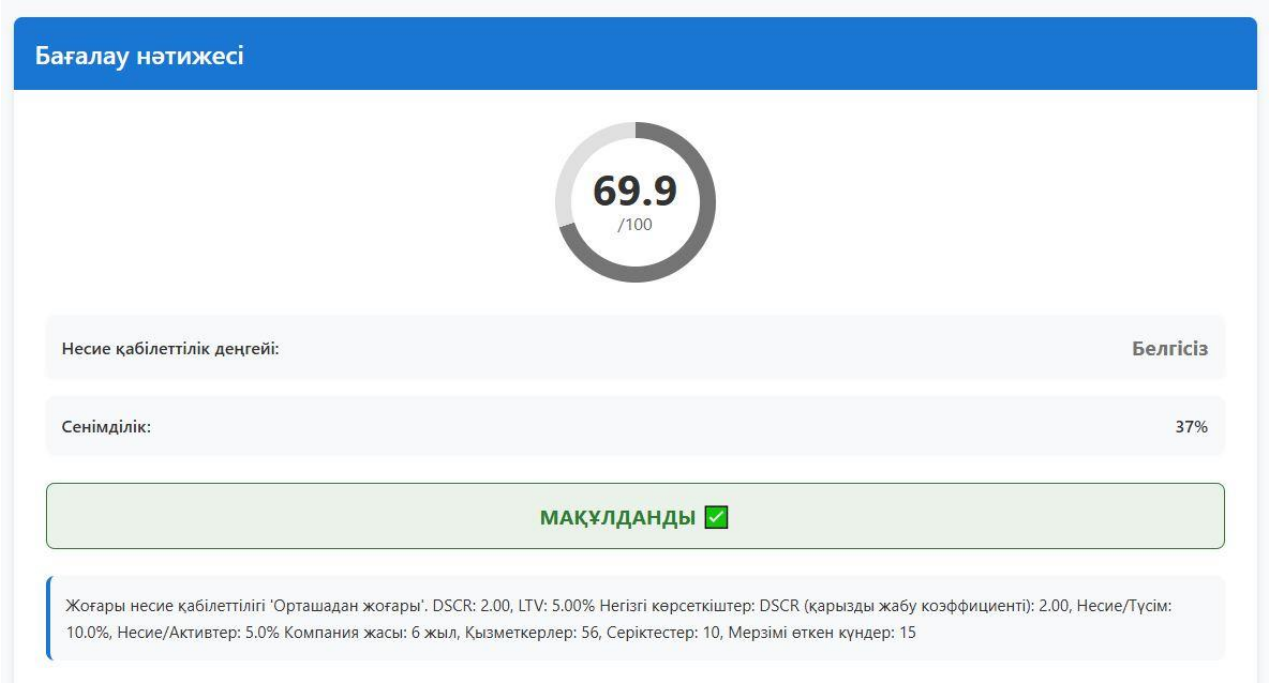
3.5 сурет – AI моделінің несие қабілеттілігін бағалау интерфейсі

Бұл деректер компанияның іскерлік тәртібі мен операциялық тәуекелдерін сипаттайды. Мысалы, көп кешіктірілген төлемдер компанияның сенімділігіне теріс әсер етуі мүмкін, ал тәжірибелі және үлкен штаты бар компаниялар керісінше, жақсы рейтинг алуға бейім.

3. Барлық деректер енгізілгеннен кейін жүйе автоматты түрде есеп жүргізіп, төмендегідей нәтижелерді шығарады және 3.6-шы суретте көрсетілген:

- Несие қабілеттілік деңгейі (рейтинг) – 0-ден 100-ге дейінгі шкала бойынша есептеледі;
- Сенімділік пайызы – модельдің бұл шешімге қаншалық сенімді екенін көрсететін көрсеткіш;
- Нәтиже статусы – мысалы, «Мақұлданды ✓» немесе «Қабылданбады ✗».

Сонымен қатар, жүйе бағалау нәтижесіне ықпал еткен барлық факторларды қысқаша сипаттап көрсетеді: мысалы, DSCR: 2.0, Несие/Түсім: 10.0%, Қызметкерлер саны: 56 адам, Мерзімі өткен күндер: 15, т.б.



3.6 сурет – AI моделінің интерфейсі

Бұл нәтиже несиелеуші ұйым үшін шешім қабылдауға арналған визуалды әрі ақпараттық анықтама ретінде қызмет етеді. Жүйе бір жағынан тәуелсіз аналитикалық құрал рөлін атқарса, екінші жағынан — пайдаланушы үшін түсінікті және сенімді есептермен қамтамасыз етеді.

ҚОРЫТЫНДЫ

Бұл жобада жасанды интеллект негізінде компаниялардың кредиттік қабілетін бағалауға арналған модель әзірленді. Модель қаржылық көрсеткіштерді талдап, компанияларға кредиттік рейтинг тағайындауға мүмкіндік береді. Жоба барысында деректерді алдын ала өңдеу, рейтингтерді санаттарға бөлу, модельді оқыту және бағалау қадамдары жүзеге асырылды. XGBoost алгоритмі негізінде құрылған модель жоғары дәлдік көрсетті және нақты болжау қабілетіне ие болды. Сонымен қатар, модельді болашақта нақты банктік жүйелерге біріктіруге болады. Жалпы алғанда, бұл шешім қаржы саласындағы процестерді автоматтандыруға және адамдық фактор әсерін азайтуға бағытталған тиімді құрал болып табылады. Жоба нәтижелері несие тәуекелін бағалау жүйелерін жетілдіруге үлес қоса алады.

Зерттеу барысында келесі нәтижелерге қол жеткізілді:

- Қаржылық және рейтингтік деректерге алдын ала өңдеу жүргізілді: жетіспейтін мәндер толтырылды, барлық белгілер масштабталды, теңгерімсіз кластар SMOTE әдісімен теңестірілді;
- Рейтингтер 6 негізгі санатқа (A+, A, BBB, BB, B, Junk) біріктіріліп, оларды сандар арқылы реттілікпен көрсетуге мүмкіндік берілді;
- Классификация міндеті үшін XGBoost алгоритмі таңдалып, гиперпараметрлері GridSearchCV арқылы оңтайландырылды;
- Модельдің дәлдігі жоғары нәтижелер көрсетті, ал қателіктер матрицасы арқылы оның жұмыс тиімділігі жан-жақты бағаланды;
- Белгілер маңыздылығы талданып, рейтингке әсер ететін негізгі қаржылық көрсеткіштер анықталды;
- Оқытылған модель мен деректерді өңдеу пайплайны болашақта қолдану үшін сақталып, практикалық интеграцияға дайын күйге келтірілді.

Жалпы алғанда, модель қаржылық рейтингтерді автоматты түрде болжау мәселесінде тиімді құрал ретінде көрінді. Бұл шешім қаржы институттары, банктер мен инвестициялық қорлар үшін несие тәуекелін бағалауды жеңілдетіп, адам факторына тәуелділікті азайтады.

Болашақта модельді жетілдіру бағыттарына келесілер жатады:

- Уақыттық қатарлар арқылы компаниялардың қаржылық динамикасын есепке алу;
- Салалық сипаттамаларды енгізу (өндіріс, сауда, қызмет көрсету және т.б.);
- Басқа ML-алгоритмдермен ансамбльдер құру арқылы модельді одан әрі тұрақтандыру;
- Веб-қосымша немесе API түрінде модельді нақты қолдануға енгізу.

Осылайша, зерттеу жұмысы барысында алға қойылған барлық ғылыми және тәжірибелік міндеттер толық көлемде орындалды. Жүргізілген талдаулар мен жасалған модельдер компаниялардың несиелік қабілеттілігін бағалаудың сапасын арттыруға бағытталып, нақты нәтижелер берді. Зерттеу нәтижелері

практикалық қызметте, атап айтқанда қаржылық тәуекелдерді басқару, автоматтандырылған шешім қабылдау жүйелерін құру және несие беру саясатын оңтайландыру салаларында кеңінен қолдануға мүмкіндік береді. Сонымен қатар, бұл жұмыс болашақ ғылыми ізденістерге, жасанды интеллект пен машиналық оқыту әдістерін қаржы саласында жетілдіруге берік әдістемелік негіз бола алады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

2 Géron, A. (2019). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. O'Reilly Media.

3 James, G., Witten, D., Hastie, T., & Tibshirani, R. (2021). An Introduction to Statistical Learning. Springer.

4 XGBoost Documentation — https://xgboost.readthedocs.io

5 scikit-learn Documentation — https://scikit-learn.org

6 Kaggle: Corporate Credit Rating Dataset — https://www.kaggle.com

7 Баймұхаметов, Е.Қ. (2018). Қаржылық талдау негіздері. Алматы: Экономика.

8 National Bank of Kazakhstan. (2022). Financial Stability Report.

9 Altman, E. I. (1968). Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy.

10 Basel Committee on Banking Supervision. (2019). Credit Risk Modelling. BIS.

11 KPMG Kazakhstan. (2021). Credit Risk in Banking: Trends and Challenges.

12 Moody’s Investors Service. (2022). Credit Rating Methodologies.

13 Standard & Poor’s (2021). Corporate Credit Rating Criteria.

14 Тусупбеков, А. (2020). Жасанды интеллект және нейрондық желілер. Алматы: Қазақ университеті.

15 Harvard Business Review (2020). How AI is Changing the Future of Credit Scoring.

16 European Banking Authority. (2020). Guidelines on Loan Origination and Monitoring.

17 OECD (2021). AI in Finance: Risks and Opportunities.

18 Gartner Report (2022). Top Trends in AI and ML for Financial Services.

19 Қазақстан Республикасы Ұлттық Банкі (2023). Цифрлық қаржы қызметтері бойынша есеп.

20 Microsoft Azure ML Docs — https://learn.microsoft.com/en-us/azure/machine-learning/

21 Statista (2023). AI Adoption in Financial Services Worldwide.

22 IBM AI for Credit Risk — https://www.ibm.com/watson/financial-services/credit-risk

23 Жүнісов, Б.Ж. (2019). Экономикалық қауіпсіздік және қаржылық тұрақтылық.

24 PyCaret Documentation — https://pycaret.org

25 Arora, A., & Rahman, A. (2020). AI-Based Credit Scoring Models: A Comparative Study.

26 Deloitte (2021). The Future of Credit Risk Modeling.

27 Финансовая академия при Правительстве РФ (2020). Методика оценки кредитоспособности заемщиков.

28 Towards Data Science (2022). Building a Credit Scoring Model Using ML.

29 Лапин, Е.В. (2021). Методы анализа финансовых коэффициентов предприятий.

30 World Bank (2022). Responsible AI and Data Use in Credit Assessment.