

әл-Фараби атындағы Қазақ ұлттық университеті

ӘОЖ 004.42(043)

Қолжазба құқығында

БАГИТОВА КАЛАМКАС БАГИТОВНА

**Онлайн әлеуметтік желілерде саяси экстремизмді анықтау әдістері
мен модельдерін әзірлеу және зерттеу**

8D06301 – Ақпараттық қауіпсіздік жүйелері

Философия докторы (PhD)
дәрежесін алу үшін дайындалған диссертация

Отандық ғылыми кеңесші:
физика-математика ғылымдарының кандидаты
Мусиралиева Ш.Ж.,
әл-Фараби атындағы Қазақ ұлттық
университеті, Алматы, Қазақстан

Шетелдік ғылыми кеңесші:
техника ғылымдарының докторы,
профессор Терейковский И.А.
Украина Ұлттық техникалық университеті, Украина

Қазақстан Республикасы
Алматы, 2023

МАЗМҰНЫ

| | |
|--|----|
| НОРМАТИВТІ СІЛТЕМЕЛЕР | 3 |
| БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР | 4 |
| КІРІСПЕ | 6 |
| 1 ОНЛАЙН ӘЛЕУМЕТТІК ЖЕЛІЛЕРІНДЕГІ САЯСИ ЭКСТРЕМИЗМДІ ТАНУ ЖҮЙЕЛЕРІН ТАЛДАУ | 13 |
| 1.1 Әлеуметтік желілерінде саяси экстремизмді анықтау мәселелері | 13 |
| 1.2 Онлайн әлеуметтік желілерінде саяси экстремистік мәтіндерді анықтау құралдарын талдау | 15 |
| 1.3 Әлеуметтік желілерінің графикалық ресурстарындағы саяси экстремистік мазмұнды анықтау құралдарын талдау | 18 |
| 1.4 Онлайн әлеуметтік желілердіне саяси экстремистік мәтіндер мен графикалық ресурстарды анықтаудағы есептің қойылымы | 21 |
| 2 ӘЛЕУМЕТТІК ЖЕЛІЛЕРІНДЕ САЯСИ ЭКСТРЕМИЗМДІ АНЫҚТАУ ПРОЦЕСТЕРІН МОДЕЛЬДЕУ | 23 |
| 2.1 Саяси экстремистік мәтіндік контентті анықтау модельдерінің классификациясы | 23 |
| 2.2 Әлеуметтік желілерінің графикалық ресурстарын өңдеу моделі | 36 |
| 2.3 Онлайн әлеуметтік желілеріндегі графикалық ресурстарды талдаудың нейрожелілік моделі | 51 |
| 3 ОНЛАЙН ӘЛЕУМЕТТІК ЖЕЛІЛЕРІНДЕ САЯСИ ЭКСТРЕМИСТІК МАЗМҰНДЫ АНЫҚТАУ ӘДІСТЕРІ | 62 |
| 3.1 Әлеуметтік желілерінде саяси экстремизмді анықтауға арналған мәтіндер корпусын құру процедурасы | 62 |
| 3.2 Онлайн әлеуметтік желілеріндегі саяси мазмұнды мәтіндік материалдарды анықтау әдісі | 67 |
| 3.3 Әлеуметтік желілерінің графикалық ресурстарында саяси экстремизмді анықтау әдісі | 73 |
| 3.4. Онлайн әлеуметтік желілеріндегі саяси экстремизмді анықтау әдісін эксперименттік тексеру | 84 |
| ҚОРЫТЫНДЫ | 94 |
| ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ | 96 |

НОРМАТИВТІ СІЛТЕМЕЛЕР

Берілген диссертацияда келесі стандарттарға сәйкес сілтемелер қолданылды:

Қазақстан Республикасы МЖМБС 5.04.034-2011. «Қазақстан Республикасы Мемлекеттік жалпыға білім беру стандарты. Жоғары оқу орнынан кейінгі білім. Докторантура». Негізгі ережелер ҚР БҒМ бекітілген. 17.06.2011 ж. №261. Астана, 2011 ж.

«Диссертацияны безендіру нұсқаулығы», Қазақстан Республикасы БҒМ ЖАК 28 қыркүйек, 2004 жыл. №377-3 ж.

ГОСТ 7.32-2001. Ғылыми зерттеу жұмысының есебі. Безендіру ережелері мен құрылымы.

ГОСТ 7.1-2003. Библиографиялық таспа. Библиографиялық сипаттау.

БЕЛГІЛЕУЛЕР МЕН ҚЫСҚАРТУЛАР

| | | |
|---------|---|---|
| CNN | – | Convolutional Neural Network |
| RNN | – | Recurrent Neural Network |
| IBM | – | International Business Machines |
| LSTM | – | Long short-term memory |
| LIWC | – | Linguistic Inquiry and Word Count |
| TF-IDF | – | Term frequency–inverse document frequency |
| ЖТН | – | Жеке тіркеу нөмірі |
| ГТД | – | Global Terrorism Database |
| START | – | Study of Terrorism and Responses to Terrorism |
| PGIS | – | Pinkerton's Global Intelligence Service |
| CETIS | – | Center for Terrorism and Intelligence Studies |
| ISVG | – | Institute for the Study of Violent Groups |
| RAND | – | Research and Development |
| RDWTI | – | RAND Database of Worldwide Terrorism Incidents |
| OSINT | – | Open Source INTelligence |
| SOCMINT | – | Social media intelligence |
| CBRNE | – | Chemical, Biological, Radiological, Nuclear, and Explosives |
| DVI | – | Disaster Victim Identification |
| AI | – | Artificial Intelligence |
| PHP | – | Hypertext Preprocessor |
| CGI | – | Common Gateway Interface |
| ASP | – | Active Server Pages |
| HTTP | – | HyperText Transfer Protocol |
| API | – | Application Programming Interface |
| VK API | – | Vkontakte Application Programming Interface |
| HTTPS | – | HyperText Transfer Protocol Secure |
| NLP | – | Natural Language Processing |
| BOW | – | Bag-of-Words |
| TF | – | Term Frequency |
| IDF | – | Inverse Document Frequency |
| KNN | – | K Nearest Neighbor |
| ROC | – | Receiver Operating Characteristic |
| AUC-ROC | – | Area Under the Curve - Receiver Operating Characteristic |
| TP | – | True Positive |
| TN | – | True Negative |
| FP | – | False Positive |
| FN | – | False Negative |
| ML | – | Machine Learning |
| СЭБ | – | Саяси экстремистік бағыт |
| ЛР | – | Логистическая регрессия |
| LASPL | – | Linguistic Analyzer of socio-psychological lexeme |

| | | |
|------|---|---------------------------------|
| DHS | – | Department of Homeland Security |
| HD | – | Human Dignity |
| CV | – | Call for Violence |
| VO | – | Offensive/Vulgar Language |
| PTV | – | Pakistan Television Corporation |
| SVM | – | Support Vector Machine |
| RF | – | Random Forest |
| POS | – | Part of Speech |
| ReLU | – | Rectified Linear Unit |
| RGB | – | Red, Blue, Green |
| GRU | – | Gated Recurrent Unit |

КІРІСПЕ

Зерттеу тақырыбының өзектілігі. Ақпараттық технологиялар қарқынды дамыған заманында "Telegram", "YouTube", "Twitter", "ВКонтакте", "Facebook" және т.с.с әлеуметтік желілерді қолданушылар саны күннен күнге артып келеді. Өртүрлі форматтағы профильдер құруға, дүниежүзілік аудиториямен байланыс орнатуға және ақпарат алмасуға мүмкіндік беретін бұл платформалар планетаның әр түкпірінен миллиондаған адамдарды бір – бірімен байланыстырады. Олар біздің өміріміздің ажырамас бөлігіне айналды, қарым – қатынас жасау, жаңа достар табу және бизнес жасау тәсілдерін өзгертті. Әлеуметтік желілердің танымалдылығының артуының негізгі себептерінің бірі – олардың қол жетімділігі. Смартфондар мен жоғары жылдамдықты интернеттің дамуымен адамдар ыңғайлы уақытта және кез – келген жерде әлеуметтік платформалардағы аккаунттарына оңай қол жеткізе алады. Бұл оларға әрдайым жаңалықтардан хабардар болуға, достары және отбасымен сөйлесуге, өз ойлары мен идеяларын өзгемен жылдам бөлісуге мүмкіндік береді. Әлеуметтік желілер қолданушыларына жаңа достар мен қызығушылық серіктестерін табуға мүмкіндік береді. Іздеу мүмкіндіктері мен қолайлы контактілерді ұсыну арқылы пайдаланушылар ортақ қызығушылықтары, хоббиі және кәсіби дағдылары бар адамдарды таба алады. Бұл оларға әлеуметтік желісін кеңейтуге және дамудың жаңа мүмкіндіктерін табуға мүмкіндік береді. Интернеттегі әлеуметтік медиа бизнес пен маркетинг үшін таптырмас құралға айналды. Брендтік беттер мен жарнамалық науқандарды құру мүмкіндігімен компаниялар өздерінің мақсатты аудиторияларына жетіп, тауарлары мен қызметтерін жарнамалай алады. Сонымен қатар, әлеуметтік медианың аналитикалық құралдарының арқасында компаниялар өз клиенттерінің мінез-құлқын талдап, маркетингтік стратегиясын оңтайландыра алады.

Дегенмен, кез келген жаңа технологиялық серпіліс сияқты, онлайн әлеуметтік желілердің де кемшіліктері мен жағымсыз жақтары бар. Деректердің құпиялылығы мен қауіпсіздігіне қатысты мәселелер онлайн әлеуметтік медиа пайдаланушыларының алдында тұрған негізгі мәселелердің бірі болып табылады. Сонымен қатар, онлайн әлеуметтік желілер экстремистерге жаңа қолдаушыларды тартуға, өз идеяларымен, яғни ақпарат алмасуға және іс – әрекеттерін жүзеге асыруға ыңғайлы алаң болып табылады [1, 2]. Осындай мысалдардың бірі – 2022 жылғы қаңтар оқиғасы. Қазақстанның батысында автомобильдерге жанармай көзі болып табылатын газ бағасының екі есе өсуінен халық арасында бейбіт наразылық митингілер басталған болатын. Республиканың батыс бөлігінде ғана емес, Қазақстанның басқа өңірлерінде де халықтың өмір сүру деңгейінің нашарлауынан, басқа да елеулі себептерге байланысты халық наразылығының өсуі сағат санап арта түсті. Бейбіт наразылық акцияларын тонаушылар, сондай-ақ экстремистер одан әрі өрбітіп, елде бүліктер орын алып, соңы адам шығынына ұшыратты. Олардың әрекеттері біреумен басқарылғаны сөзсіз. Экстремисттік іс – әрекеттің басты мақсаты Қазақстандағы

билікті құлатып, басып алу болды. Осы белең алған тәртіпсіздіктің бірден бір құралы – әлеуметтік желілер болғаны сөзсіз.

Интернеттегі әлеуметтік желілерде экстремизммен күресу маңызды, міндетті және қиын мәселенің бір болғанымен, шешімі бар тапсырма қатарына жатқызуға болады. Саяси экстремизмді анықтау және алдын алу үшін тиімді жүйелер мен модельдерді дамыту елдегі қауіпсіздік пен тұрақтылықты қамтамасыз етудің негізі болып табылады. Сәйкесінше, аталған сала бойынша ғылыми зерттеулер жүргізуді, сол арқылы экстремизмнің кез келген көріністерін анықтауға, алдын алуға және жолын кесуге бағытталған тиімді және уақтылы шаралар кешенін жүзеге асыруды талап етеді.

Мәселе Бүкіләлемдік сипатқа ие және көптеген елдер үшін, соның ішінде Қазақстан үшін өте өзекті болып табылады.

Интернет ақпараттық кеңістігі әр түрлі ресурстардан тұрады. Сонымен бірге олардың басым көпшілігі бұқаралық ақпарат құралдары болып табылмайды, нәтижесінде бұқаралық ақпарат құралдары туралы заңнаманың нормаларын қолдану мүмкін болмайды. Экстремизм идеяларының таралуына қарсы тұру үшін қазіргі уақытта құқық қорғау органдары қылмыстық заңнаманың «Экстремизмге қарсы іс-қимыл туралы Қазақстан Республикасының 2005 жылғы 18 ақпандағы №31 Заңы» [3] нормасы, «Қазақстан Республикасында діни экстремизм мен терроризмге қарсы іс-қимыл жөніндегі 2018 – 2022 жылдарға арналған мемлекеттік бағдарламаны бекіту туралы», Қазақстан Республикасы Үкіметінің 2018 жылғы 15 наурыздағы № 124 қаулысы [4] пайдаланылады.

Қазіргі таңда Қазақстан аумағында тыйым салынған террористік құрылымдардың ұлттық тізіміне 22 ұйым енгізілген [5].

2020 жылдың қарашасында ҚР президенті Қ.К.Тоқаев ШЫҰ-ға мүше мемлекеттерді сепаратизм, терроризм мен экстремизммен күреске бағытталған Ақпараттық қауіпсіздік орталығын құруға шақырды [6].

Аталған мәселелерді Қазақстан Республикасының ұлттық қауіпсіздігіне төнетін қатер ретінде қарастыруға болады. Интернеттегі экстремистік іс-әрекеттерге қарсы іс-қимыл саласындағы ахуал күрделі болып қала береді, бұл ғылыми зерттеулер жүргізуді және экстремизмнің кез-келген көріністерін анықтауға, алдын алуға және жолын кесуге бағытталған тиімді және уақтылы шаралар кешенін жүзеге асыруды қажет етеді.

Сонымен қатар, экстремизмді зерттеуші сарапшылар жаһандық коронавирустық пандемия салдарынан Интернетте көп уақыт отыруға мәжбүр болған азаматтардың экстремистік ұйымдар үшін осал тұс екенін көрсетеді және аталған факторлардың үйлесуі зорлық-зомбылық экстремизмі мен терроризмнің өсуіне әкеледі деп болжам жасайды [7-9].

Жоғарыда келтірілген тұжырымдарты ескере отырып, веб-ресурстардағы қазақ тіліндегі экстремистік бағыттағы мәтіндерді анықтауға арналған модельдерді құру тапсырмасы **аса өзекті** деген қорытындыға келуге болады.

Зерттеу жұмысының мақсаты. Онлайн әлеуметтік желілеріндегі мәтіндік және графикалық ресурстарда саяси экстремизмді тиімді анықтаудың модельдері мен әдістерін зерттеу және әзірлеу

Зерттеудің міндеттері. Қойылған мақсатқа қол жеткізу үшін келесі міндеттерді орындау қарастырылады:

1. Онлайн әлеуметтік желілерде саяси экстремизм белгілерін көрсететін қазақ тіліндегі экстремистік мәтіндер корпусын әзірлеу;
2. Онлайн әлеуметтік желілерде қазақ тіліндегі саяси экстремизм мәтіндерін анықтау үшін әдістер мен модельдерді әзірлеу;
3. Саяси экстремизмді анықтау үшін онлайн әлеуметтік желілердің графикалық ресурстарын өңдеу және нейрондық талдау модельдерін әзірлеу;
4. Онлайн әлеуметтік желілердің графикалық ресурстарында саяси экстремизмді анықтаудың нейрондық әдісін әзірлеу;
5. Әзірленген шешімдерді эксперименттік тексеру.

Зерттеу нысаны. Онлайн әлеуметтік желілердің мәтіндік және графикалық ресурстарында саяси экстремизмді анықтау процестері.

Зерттеу пәні. Онлайн әлеуметтік желілердің мәтіндік және графикалық ресурстарында саяси экстремизмді анықтаудың модельдері мен әдістері.

Зерттеу әдісі. Зерттеу әдісі ретінде Машиналық және терең оқыту әдістері, мәтіндерді, бейнелерді жіктеу әдістері, табиғи тілді өңдеу әдістері, нейрондық желілер, әлеуметтік желілерді талдау әдістері, статистикалық өңдеу әдістері, жүйелік талдау әдістері қолданыс тапты.

Алынған нәтижелердің ғылыми жаңалығы:

1) TF-IDF және әлеуметтік-психологиялық лексемдерлі талдау процедураларын аралас қолдану арқылы қазақ тілді мәтіндердегі саяси экстремизмді анықтаудың дәлдігін арттыру мүмкіндігін қамтамасыз ететін LSTM желісінің кіріс өрісін қалыптастыру әдісі әзірленді;

2) Стемминг процедурасы мен модификацияланған SpellChecker емлені түзету алгоритмін қолдану арқылы қазақ тілді мәтіндердегі саяси экстремизм мазмұнын анықтаудың дәлдігін арттыру мүмкіндігін қамтамасыз етуге арналған алдын ала өңдеу әдісі әзірленді

3) Саяси экстремизм мазмұнын көрсете отырып, онлайн әлеуметтік желілерде саяси экстремизмді анықтаудың модельдері мен әдістерін әзірлеуге мүмкіндік беретін қазақ тіліндегі мәтіндер корпусы әзірленді;

4) Типтік кедергілерді сүзу үшін вейвлет түрлендіру аппаратын және суреттердің жарықтығы мен контрастын түзету үшін әзірленген математикалық аппаратты пайдаланудың ұсынылған тәсілінің арқасында онлайн әлеуметтік желілердің графикалық ресурстарын нейрондық желілік талдаудың дәлдігін арттыруға мүмкіндік беретін онлайн әлеуметтік желілердегі бейнелер мен бейнематериалдарды алдын ала өңдеу моделі әзірленді;

5) Құрылымы конволюциялық және рекурренттік нейрондық желілердің архитектуралық параметрлеріне негізделіп, онлайн әлеуметтік желілердің

суреттері мен бейнематериалдарында саяси экстремизмді анықтаудың тиімді әдісін жасауға мүмкіндік беретін нейрондық желіні талдау моделі әзірленді;

б) Ұсынылған алдын ала өңдеу және нейрондық желіні талдау үлгілерін пайдалану арқылы нейрондық желі моделінің кіріс өрісін графикалық ресурстар өлшемдерінің өзгергіштігіне бейімдеуге ұсынылған тәсіл арқылы онлайн әлеуметтік желілердегі кескіндер мен бейнематериалдардағы саяси экстремизмді анықтау дәлдігін арттыру мен ресурс сыйымдылығын азайтуды қамтамасыз ететін, онлайн әлеуметтік желілердегі бейнелер мен бейнематериалдардағы саяси экстремизмді анықтау әдісі әзірленді.

Жұмыстың теориялық маңыздылығы. Диссертациялық жұмыстың теориялық маңыздылығы саяси экстремистік іс-әрекеттер мен ұйымдарды анықтау әдістері мен алгоритмдері саласындағы білім жиынтығына негізделген. Алынған іргелі нәтижелерді әлемдік ғылыми қауымдастық пайдалана алады.

Жұмыстың практикалық маңыздылығы. Әзірленген әдістің нәтижелерін ақпараттық қауіпсіздікті, сыни инфрақұрылымды қамтамасыз ету, интернет – экстремизммен күрес жөніндегі уәкілетті органдар пайдалануы мүмкін.

Қорғауға шығарылатын негізгі тұжырым. Машиналық оқыту әдістерін оқытуға және тестілеуге арналған қазақ тіліндегі экстремистік мәтіндер корпусы құрастырылды. Әлеуметтік желілеріндегі қазақ тіліндегі саяси экстремистік бағыттағы мәтіндерді анықтауға арналған талдау моделі құрастырылды. LSTM моделіне алдын ала стемминг алгоритмі орындалған мәтін ендірудің TF-IDF әдісін қолдану арқылы әлеуметтік желілеріндегі қазақ тіліндегі экстремистік мәтіндерді анықтау тапсырмасының дәлдігін арттыруға болатындығы анықталды. Алдын ала өңдеу және нейрондық желіні талдау үлгілерін пайдалану арқылы, сондай – ақ нейрондық желі моделінің кіріс өрісін графикалық ресурстар өлшемдерінің өзгергіштігіне бейімдеуге ұсынылған тәсіл арқылы онлайн әлеуметтік желілердегі кескіндер мен бейнематериалдардағы саяси экстремизмді анықтау әдісі әзірленді.

Сенімділік дәрежесі мен апробациялау нәтижелері. Зерттеудің сенімділігі мен нәтижелерінің негізділігі міндеттерді қоюдың негізделген жауапкершілігімен, критерийлердің және берілген саладағы зерттеулердің жай-күйінің сарапталуымен, жүргізілген эксперименттер санының көптігімен, сондай-ақ олардың практикаға табысты енгізілуімен қамтамасыз етіліп дәйектеледі. Диссертация нәтижелері төмендегі ғылыми журналдар мен конференция материалдарында жарияланды:

Қазақстан Республикасы Ғылым және жоғары білім министрлігі Білім және ғылым саласындағы бақылау комитеті ұсынатын журналдардағы мақалалар:

1. K. Bagitova, I. Tereikovskiyi, I. Babayev, L. Tereikovska, O. Tereikovskiyi. Model for processing images of online social networks used to recognize political extremism. DOI: <https://doi.org/10.26577/JMMCS2023v119i3a8> Vol. 118 No. 2

(2023): Journal of Mathematics, Mechanics and Computer Science (**indexed in Web of Science**).

2. Ш.Ж. Мусиралиева, М.А. Болатбек, М. Сағынай, Ж.Ы. Елтай, К.Б. Багитова. Экстремистік мәліметтер түсінігі және экстремизмге қарсы күрес жобаларына жүйелік шолу. NEWS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN PHYSICO-MATHEMATICAL SERIES ISSN 1991-346X Volume 3. Number 347 (2023). 112–130. <https://journals.nauka-nanrk.kz/physics-mathematics/article/view/5792/4039>

3. Багитова К.Б., Мусиралиева Ш.Ж., Болатбек М.А., Оспанов Р.К. Разработка программного обеспечения ExWeb для выявления экстремистского контента в сети Интернет. УДК 004.056.5. «Известия НАН РК. Серия физика и информатики». ISSN 2518-1726 (Online), ISSN 1991-346X (Print). SERIES PHYSICS AND INFORMATION TECHNOLOGY 2 (346) APRIL – JUNE 2023. Стр. 81 – 95.

<https://journals.nauka-nanrk.kz/physics-mathematics/article/view/5414/3871>

4. М.А. Болатбек, К.Б. Багитова, Ш.Ж. Мусиралиева. Киберқауіпсіздік мәселелерін табиғи тілді өңдеу әдістері арқылы шешу тақырыбына жүйелік шолу. NEWS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN PHYSICO-MATHEMATICAL SERIES ISSN 1991-346X VOLUME 3, NUMBER 343 (2022), 52-70. <https://journals.nauka-nanrk.kz/physics-mathematics/article/view/4690/3560>

5. М.А. Болатбек, Ш.Ж. Мусиралиева, К. Багитова, А.Т.Нюсупов, Е. Абайұлы. Веб-ресурстардағы фишингтік хабарламалар және оларды машиналық оқыту әдістері арқылы анықтау. NEWS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN PHYSICO-MATHEMATICAL SERIES ISSN 1991-346X Volume 4, Number 344 (2022), 16-29. <https://journals.nauka-nanrk.kz/physics-mathematics/article/view/4789/3655>

Скопуста индекстелетін журналдардағы ғылыми мақала:

1. Shynar Mussiraliyeva, Kalamkas Bagitova and Daniyar Sultan, “Social Media Mining to Detect Online Violent Extremism using Machine Learning Techniques” International Journal of Advanced Computer Science and Applications (IJACSA), 14(6), 2023. <http://dx.doi.org/10.14569/IJACSA.2023.01406146>

Халықаралық конференция материалдарындағы мақалалар:

1. Ш.Ж. Мусиралиева, К.Б. Багитова, И.А. Терейковский, А.М. Усманова. Әлеуметтік желілердегі суреттер мен бейнелерді өңдеудің ерекшеліктері VIII - международная научно-практическая конференция «Информатика и прикладная математика», 26-27 октября 2023 года, Алматы, Казахстан, 305 – 310 стр.

2. S. Toliupa, I. Tereikovskiy, L. Tereikovska, S. Mussiraliyeva and K. Bagitova, "Deep Neural Network Model for Recognition of Speaker’s Emotion," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 172-176, doi: 10.1109/PICST51311.2020.9468017. <https://ieeexplore.ieee.org/document/9468017>

3. Mussiraliyeva, S., Bolatbek, M., Omarov, B., Bagitova, K. Detection of Extremist Ideation on social media Using Machine Learning Techniques. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020, 12496 LNAI, стр. 743–752 (scopus indexed, процентиль 50) https://link.springer.com/chapter/10.100/978-3-030-63007-2_58 12th International Conference, ICCCI 2020, Da Nang, Vietnam, November 30 – December 3, 2020, Proceedings

Зерттеушінің жеке үлесі. Ізденуші диссертациялық жұмыстың қойылған міндеттерін шешті. Онлайн әлеуметтік желілердегі қазақ тіліндегі саяси экстремистік бағыттағы мәтіндерді және графикалық ресурстарды анықтаудың моделі мен әдісі әзірленді. Машиналық оқыту алгоритмдерін оқыту мен тестілеуге арналған қазақ тіліндегі саяси экстремистік мәтіндер корпусы құрастырылды. Саяси экстремизмді анықтау үшін онлайн әлеуметтік желілердің графикалық ресурстарын өңдеу және нейрожелілік талдау моделі әзірленіп, нейрондық әдісі жасалды. Әзірленген модель мен әдістің дәлдігін анықтау мақсатында эксперименттер жүргізілді.

Диссертация тақырыбының ғылыми-зерттеу жұмыстарының жоспарларымен байланысы. Берілген жұмыс Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің тапсырысы бойынша «Әлеуметтік желілердегі экстремистік мазмұнды анықтау модельдерін және әдістерін құрастыру» жобасының ғылыми-зерттеу жұмыстарының аясында орындалды, ЖТН АР15473408. Басым бағыт: Ұлттық қауіпсіздік және қорғаныс. Мамандандырылған бағыт: Ақпараттық қауіпсіздікті қамтамасыз ету.

Басым бағыт: Ұлттық қауіпсіздік және қорғаныс

Мамандандырылған бағыт: Ақпараттық қауіпсіздікті қамтамасыз ету

Нәтиженің жарияланымдары. Диссертацияның ғылыми ережелері мен тұжырымдарына негізделген міндеттер толығымен орындалған. Жұмыс нәтижелері 10 ғылыми жұмыста жарияланды: оның ішінде Scopus дерекқорына кіретін нөлдік емес импакт-факторы бар журналдарда 1 мақала, *Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым және жоғары білім саласындағы сапаны қамтамасыз ету комитеті* ұсынған журналдарда 5 мақала және халықаралық конференциялар материалдарында 3 мақала.

Диссертацияның құрылымы мен көлемі. Диссертация 103 бетте жазылған кіріспеден, үш бөлімнен, қорытындыдан тұрады және 59 суреттен, 12 кестеден, 89 пайдаланылған дереккөзден тұрады.

Кіріспеде диссертациялық жұмыс тақырыбы өзектілігінің негіздемесі берілген. Ғылыми – зерттеу жұмысының мақсаты, нысаны және пәні тұжырымдалған. Сонымен бірге, ғылыми жаңалығы және тәжірибелік маңызы көрсетілген. Зерттеу жұмыстарының нәтижелері және жарияланымдары туралы мәліметтер келтірілген.

Бірінші бөлімде экстремизм түсінігі және жіктелуі, онлайн әлеуметтік желілеріндегі саяси экстремистік мәтіндерді және графикалық ресурстарды анықтау құралдарын талдау қарастырылады.

Екінші бөлімде саяси экстремистік мәтіндік контентті анықтау модельдерінің классификациясы, әлеуметтік желілерінің графикалық ресурстарын өңдеу моделі мен талдаудың нейрожелілік моделі сипатталған.

Үшінші бөлімде әлеуметтік желілерінде қазақ тіліндегі саяси экстремистік мәтіндерді және графикалық ресурстарды анықтау есебі үшін түрлі машиналық оқыту әдістері мен ұсынылатын әдіске салыстырмалы талдаулар жүргізіледі.

Қорытындыда жұмыстың негізгі қорытындылары мен нәтижелері тұжырымдалады.

1 ОНЛАЙН ӘЛЕУМЕТТІК ЖЕЛІЛЕРІНДЕГІ САЯСИ ЭКСТРЕМИЗМДІ ТАҢУ ЖҮЙЕЛЕРІН ТАЛДАУ

1.1 Әлеуметтік желілерінде саяси экстремизмді анықтау мәселелері

Web 2.0 ортақ идеясымен біріктірілген интернет пен әлеуметтік қызметтердің қарқынды дамуы мен кеңеюі зерттеу қызығушылықтарының жаңа саласын, яғни виртуалды немесе онлайн қауымдастықтар деп аталатын интернеттегі әлеуметтік желілерді құруға түрткі болады. Әлеуметтік медиа қолданушыларының түрлі әрекеттерінен, яғни электрондық пошта сервистерін қолдану, чаттар, блогтар құру, гиперсілтемелермен байланысты үй беттерінен ақпарат алу, медиа алмасу жүйесінде фотосуреттер мен бейнежазбаларды өңдеп, бөлісу секілді әртүрлі процестер жиынтығынан құралған. Global Digital 2023 есеп беруінің басты нәтижелері бойынша:

- 2022 жылдың 15 қарашасында әлем халқы 8 миллиардтан асып, 2023 жылдың басында 8,01 миллиардқа жетті.

- 2023 жылдың басында 5,44 миллиард адам ұялы телефондарды пайдаланады, бұл бүкіл әлем халқының 68% құрайды.

- Әлем халқының 64,4% интернетке қол жеткізе алады. Бір жыл ішінде олардың саны 1,9%-ға өсті.

- 2023 жылдың басында әлеуметтік желілерде 4,76 миллиард пайдаланушы бар, бұл әлем халқының 60%-ға жуығы.

Бұл статистикаға сүйенсек, әлеуметтік медиа әлемнің көптеген елдерінде байланыс орнату көзі, соның ішінде экстремистік көзқарастарды тарату үшін әлеуметтік желілер платформаларын пайдаланатын қолданушылар үшін ыңғайлы алаңға айналып барады.

Экстремизм түсінігі.

Экстремизм – әлеуметтік, нәсілдік, ұлттық немесе діни араздықты қоздыру; адамның әлеуметтік, нәсілдік, ұлттық, діни немесе тілдік тиесілігіне немесе дінге көзқарасына қарай оның айрықшалығын, артықшылығын немесе төмендігін насихаттау.

Экстремистік (террорлық) сипаттағы әрбір қылмыстың астарында оны жасаған адамдардың белгілі бір идеологиялық көзқарастары мен сенімдері жатыр. Оның үстіне мұндай қылмыстардың абсолютті көпшілігі топта жасалады, ал оның өкілдеріне тән идеология оның шекарасынан әлдеқайда асып түседі және экстремистік (террористік) бағыттағы ауқымды бірлестіктердің құрылуы мен қызмет етуіне негіз болады. Осыған орай, жоғарыда аталған бірлестіктердің негізгі идеологиялық бағыттарын анықтап, олардың кейбір ерекшеліктерін анықтауға болатын сияқты.

Зорлық-зомбылық экстремизм мен терроризмге қарсы тұру бойынша халықаралық аренада жасалып жатқан күш-жігермен қатар, Қазақстанда осы бағыттағы негізгі құжаттар әзірленді. Әрине, стратегия жан-жақты және мүдделі

тараптарды, заңнаманы және жұмыс салаларын ескеретін көптеген әртүрлі жұмсақ және қатты компоненттерді қамтиды.

Сонымен, Қазақстан Республикасының «Экстремизмге қарсы күрес туралы» Заңына сәйкес Қазақстанда экстремизмнің үш түрі бар [10]. Олар:

- *Саяси экстремизм* – конституциялық құрылысты күштеп өзгерту, Қазақстан Республикасының егемендігін, оның аумағының тұтастығын, қол сұғылмауын және ажырамастығын бұзу, мемлекеттің ұлттық қауіпсіздігі мен қорғаныс қабілетіне нұқсан келтіру, билікті күштеп басып алу немесе билікті күштеп ұстап тұру, құру, заңсыз әскерилендірілген құрамды басқару және оған қатысу, қарулы көтеріліс ұйымдастыру және оған қатысу, әлеуметтік және таптық араздықты қоздыру;

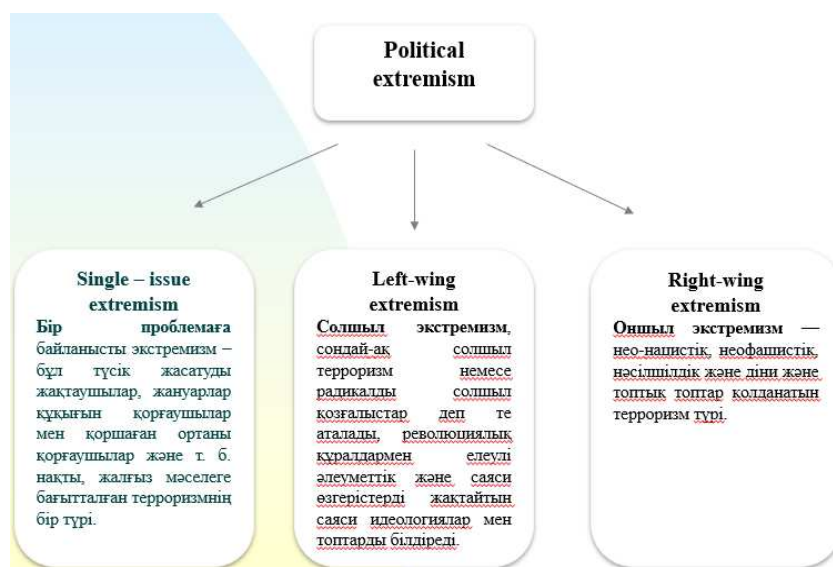
- *Ұлттық экстремизм* – нәсілдік, ұлттық және рулық араздықты қоздыру, оның ішінде зорлық-зомбылық немесе зорлық-зомбылыққа шақыру;

- *Діни экстремизм* – діни араздықты немесе алауыздықты қоздыру, оның ішінде зорлық-зомбылықпен немесе зорлық-зомбылыққа шақырумен байланысты, сондай-ақ азаматтардың қауіпсіздігіне, өміріне, денсаулығына, имандылығына немесе құқықтары мен бостандықтарына қатер төндіретін кез келген діни тәжірибені пайдалану;

Өзге елдерде, соның ішінде Еуропа елдерінде саяси идеологияның бағытына сүйене отырып, біз «сол» экстремизм (left extremism) және «оң» экстремизмді (right extremism) шартты түрде ажырата аламыз [11].

«Солшыл» экстремизм революцияшылдық, анархизм идеяларын алады, өзін еңбекші бұқараның, барлық аз қамтылғандар мен кедейлердің ең дәйекті өкілі және қорғаушысы деп жариялайды.

Олардың сынының объектілері – әлеуметтік теңсіздік, жеке адамды басып-жаншу, қанау, қоғамдағы бюрократизация. Олар бұл құбылыстарды кез келген әдіспен, соның ішінде қарулы көтерілістермен жоюға дайын.



Сурет 1.1 – Саяси экстремизмнің жіктелуі

«Оңшыл» экстремистер (фашистік, неофашистік, әсіре оңшыл, ұлтшыл, нәсілшіл қозғалыстар) қазіргі қоғамды «тәртіптің жоқтығы», «плутократияның үстемдігі», «моральдың құлдырауы», өзімшілдік үшін сынады. Оңшыл экстремистер прогрессивті қоғамдық ұйымдармен және саяси қайраткерлермен күресу үшін жиі пайдаланылады. Олардың көпшілігі мемлекеттің атын жамылып жұмыс істейді.

Әлеуметтік желілер экстремизмге қалай әсер етеді. Әлеуметтік медиа мен саяси поляризация арасындағы байланыс ұлттық қауіпсіздік шенеуніктерінің алаңдаушылығын тудыруда, олар бүкіл әлемде жалғасып жатқан экстремизм (терроризм) қауіпі туралы ескертеді. 2022 жылы АҚШ Ішкі қауіпсіздік департаменті (DHS) жалған ақпарат пен қастандық теорияларын тарататын желідегі белсенділікке байланысты «жоғары қауіпті ортаны» сипаттады.

Әлеуметтік желілерді экстремизмде (терроризмде) пайдалану. Әлеуметтік желідегі қоқан-лоққылар саяси экстремизмді қоздырумен қатар, АҚШ-қа зиянын тигізгісі келетін шетелдік және отандық ұйымдардан да келуі мүмкін. DHS мәліметтері бойынша, бұл «қауіпті субъектілер» терроризмді тудыруы мүмкін нанымдарды насихаттау үшін экстремистік хабарламаларды жиі ұсынады немесе таратады.

Бұған қоса, жаһандық лаңкестік ұйымдар өздерінің әрекет деңгейін арттыруға, жаңа ізбасарлар тартуға және әлеуметтік желілер арқылы мынадай тактикалар арқылы үрей тудыруға тырысты:

- Біз жоспарларымызды жариялаймыз;
- Әлеуметтік желі қолданушыларын желідегі қарым-қатынасқа тарту;
- Жас аудиторияны тартатын хабарламаларды пайдалану;
- Зорлық-зомбылық әрекеттерін көрсету;
- Террорлық әрекеттер үшін жауапкершілікті өз мойнына алу;
- Әлеуметтік желі пайдаланушыларын өздерінің топтық сайттарына қайта бағыттау;
- Қаржыландыруды табу.

Әлеуметтік желілер платформалары контент мазмұнын шектеу үшін әрекет ететеді, нәтижесінде экстремисттер олардың әрекеттерін одан әрі өз пайдаларына жаратып жатады. Мұндай экстремисттік топтарға жаңа пайдаланушы атын жасау арқылы әлеуметтік желі платформаларының тыйымдарын айналып өту оңай. Сондай-ақ, олар өздерінің көрінуін арттыру үшін тренд сөздерді немесе хэштегтерді қосу арқылы әртүрлі алгоритмдерді өз мүддесіне пайдаланады.

1.2 Онлайн әлеуметтік желілерінде саяси экстремистік мәтіндерді анықтау құралдарын талдау

Үгіт-насихат, радикалдандыру және өз идеяларына тарту сияқты экстремистік мәтіндер мен сөйлеудің әрбір түрінің өзіндік ерекшеліктері мен салдары бар. Олар да [12] түсіндіріледі. Әлеуметтік желілердің ауқымы үнемі

кеңейіп жатқандықтан, экстремистік ұйымдар әлеуметтік желі платформаларын үгіт-насихат тарату, адамдарды радикалдандыру және оларды зорлық-зомбылық әрекеттеріне тарту үшін пайдаланады. Сондықтан әлеуметтік желілерде экстремизмнің таралуын шектеу үшін үгіт-насихат, радикалдандыру және өз идеяларына тартуды анықтау құралын әзірлеу қажеттігі туындайды [13]. Әлеуметтік желілеріндегі мәтіндердегі экстремистік мазмұнды зерттеу келесі қиындықтарға тап болады:

1. Экстремизм туралы мәтіндер бойынша жалпыға қолжетімді деректер жиынтығының болмауы.
2. Экстремизм туралы мәтінде идеологиялық тәуелсіз және теңдестірілген деректер жиынтығының болмауы.
3. Деректер сапасын тексеру үшін автоматтандырылған деректерді тексеру әдістерінің болмауы.
4. Интернетте экстремистік мәтіндерді анықтаудың дәл автоматтандырылған әдістерінің болмауы.
5. Экстремистік мазмұнды радикалдандыру, үгіт-насихаттау және жалдау сияқты санаттарға бөлу бойынша жұмыстың шектелуі.

Онлайн әлеуметтік желілерінде саяси экстремистік мәтіндерді анықтау құралдарын талдауға сәйкес жұмыстарына шолу.

Кеннеди [14] Gab әлеуметтік желісінен 27 000 жазба жинады. Gab әлеуметтік желісі сөз бостандығын сақтаймыз деп, жеккөрінішті сөздер тарайтын баспанаға айналды. Авторлар жазбаларды адам қадір-қасиетіне шабуыл (HD), зорлық-зомбылыққа шақыру (CV) және қорлау/дөрекі тіл (VO) деп бөледі. Авторлар әрі қарай HD және түйіндемені жасырын, айқын, нәсілдік/этникалық, ұлт, жыныс, дін, жыныстық бағдар, идеология, саяси идеология және психикалық/дене саулық деп санайды. Жіктеу үшін авторлар үш классты қарастырды: HD, VO және жек көру (HD және CV комбинациясы).

Аббар және басқалар [15] 13 369 лаңкестікке қарсы твиттер, 16 506 лаңкестікке қарсы емес твиттер және 38 617 кездейсоқ твиттер жинады. Дегенмен, авторлар твиттерді жинау үшін пайдаланылатын ешбір бастапқы тіркелгілерді немесе терроризмге қатысты кілт сөздерді атап өтпеді және жиналған деректер жинағына деректерді тексеру әдістерін қолданбаған.

Асиф және басқалар [16] экстремистік мәтіндерді жинау үшін PTV news, Dawn және Geo сияқты ақпарат агенттіктерінің Facebook парақшаларын пайдаланды. Барлығы 19 497 пост жиналды, оның 5 279-ы орташа, 6 912-і өте төтенше, 2 991-і төмен экстремалды және 4 315-і бейтарап деп бағаланды. Авторлар 109 кездейсоқ қатысушыларды қамтитын сауалнамаға негізделген тестті пайдаланды. Дегенмен, авторлар барлық деректерді көрсетпеуі мүмкін 25 хабарлама үлгісін ғана пайдаланды.

Зерттеушілер әсіре оңшыл ақтардың үстемдігінің идеологиясы туралы мәліметтерді әртүрлі көздерден және орындардан жинады. Джеки мен Де Смедт [17] Германиядағы әсіре оңшыл идеологияны қолдады деп күдіктенген 100-ге жуық Twitter пайдаланушысынан 50 000 твиттер жинады. Авторлар сонымен

қатар 50 000 бейтарап твиттер жинады. Авторлар деректерді тексеру әдістері туралы ешқандай мәлімет бермеді.

Қолданыстағы экстремизм деректерінің желідегі проблемалары. Интернеттегі экстремизмнің мәтіндік деректер жинағы әртүрлі зерттеу олқылықтарын көрсетеді. Интернеттегі экстремизмнің мәтіндік деректер жиынтығында келесі мәселелер байқалады:

Мәліметтердің теңгерімсіздігі және екілік классификациясы.

Деректер теңгерімсіздігі экстремизмнің онлайн деректер жиыны үшін негізгі проблема болып табылады. Экстремизм туралы деректер жалпы әлеуметтік медиа деректерінің бір бөлігін ғана білдіретіндіктен, теңдестірілген класс деректер жинағын жасау қиынға соғады.

Деректер жиынтығының тағы бір мәселесі - экстремизм деректерінің екілік немесе ең көп дегенде үш класты классификациясы. Оның үстіне экстремизмнің көріністері күрделі және уақыт өте өзгеріп отырады. Сондықтан экстремистік мәтіндердің контекстіне негізделген категориялар құру қажет.

Тіл. Түрлі идеологиялардағы экстремизм әртүрлі тілдерде таралады. Осылайша, экстремистік мәтінді анықтау қиындай түседі. Зерттеушілердің көпшілігі ағылшын тілін ғаламдық тіл ретінде пайдаланады. Экстремист өзінің идеологиясын бүкіл әлемге тарату үшін ағылшын тілін кеңінен қолданады.

Ескірген деректер жинағы.

Стандартты деректер жиындары ескірген. Ескі деректер жиынын жаңартуды мүмкін етпейтін әлеуметтік желілердің қатаң деректер алмасу саясаты. Бұл қатаң деректерді ортақ пайдалану саясаты стандартты деректер жиынының аз болуының себептерінің бірі болып табылады.

Тексеру. Көптеген зерттеушілер бағалаушылар арасындағы келісімді қолмен тексеруді пайдаланады. Барлық деректерді қолмен тексеру мүмкін болмағандықтан, деректерді тексеру үшін кездейсоқ үлгілердің аз саны пайдаланылады. Осылайша, біржақтылық бейсаналық түрде енгізіледі.

Деректер сапасын бағалау. Интернеттегі экстремизмді зерттеген кезде, зерттеушілер көбінесе өз деректерін жинайды [18, 19]. Әлеуметтік медиа шектеулеріне және басқа мәселелерге байланысты бұрынғы пайдаланушы деректер жиыны жалпыға қолжетімді емес. Осылайша, деректер жиынын салыстыру экстремизмді онлайн зерттеуде үлкен мәселе болып табылады. Бұл да нәтижелерді салыстырудағы басқа мәселеге әкеледі. Ешбір зерттеу бірдей деректер жиынтығын пайдаланбағандықтан, экстремизмді онлайн анықтауды зерттеуде әртүрлі әдістер мен тәсілдерді қолдану арқылы алынған нәтижелерді салыстыру қиынға соғады.

Блокталған аккаунттар. Әлеуметтік медиа платформаларында зорлық-зомбылық пен өшпенділік сөздеріне қарсы қатаң саясат бар [20, 21]. Осылайша, осындай радикалды идеологиясы бар көптеген аккаунттар бірден бұғатталады. Осылайша, деректерді жинағаннан кейін де басқа зерттеушілер бұғатталған тіркелгілердің болмауына байланысты нәтижелерді шығара алмайды.

1.3 Әлеуметтік желілерінің графикалық ресурстарындағы саяси экстремистік мазмұнды анықтау құралдарын талдау

Онлайн әлеуметтік желілерде жарияланатын жалғыз бейнересурстардан саяси экстремизм мазмұнын анықтау күрделі мәселе болып табылады. Сондықтан мәтіндерге графикалық ресурстар қосымша ретінде жүреді деп есептелді. Сәйкесінше зерттеу барысында көптеген ғылыми жұмыстар мен жазбаларға шолу жасалған болатын. Бұл шолудың негізгі мақсаты – бейне зорлық-зомбылықты анықтау әдістеріне терең жүйелі шолу жасау. Соңғы онжылдықта бейне зорлық-зомбылық пен агрессивті мінез-құлықты анықтаудың әртүрлі әдістері жасалды. Бұл әдістерді жіктеу, талдау және жинақтау қажет. Бұл жүйелі шолудың негізгі ғылыми тармақтары төмендегідей сипатталған:

- Зорлық-зомбылықты анықтаудың заманауи әдістеріне шолу, олардың өзіндік ерекшелігін, негізгі ерекшеліктері мен шектеулерін көрсету;
- Бейнелердегі зорлық-зомбылықты анықтау үшін бейне мүмкіндіктері дескрипторларының рейтингі мен маңыздылығы туралы зерттеу;
- Бейне зорлық-зомбылықты анықтау үшін деректер жинақтары мен бағалау критерийлерін зерттеу;
- Бейнеге негізделген зорлық-зомбылықты анықтаудың шектеулері, қиындықтары және ашық сұрақтары туралы талқылау.

Іс-әрекетті тану. Іс-әрекетті тану – адамның іс-әрекетін анықтай алатын технология. Адамның іс-әрекеті іс-әрекеттің күрделілігіне және әрекетке қатысатын дене мүшелерінің санына қарай төрт топқа бөлінеді. Қимылдар, әрекеттер, өзара әрекеттесу және топтық әрекеттер төрт санатқа жатады. Қимыл – белгілі бір хабарды жеткізу үшін қолмен, баспен немесе дененің басқа бөліктерімен жасалған қозғалыстар қатары. Бір адамның іс-әрекеті көптеген ым-ишараның жиынтығы болып табылады. Өзара әрекеттестік – кем дегенде екі адам қатысатын адам әрекеттерінің жиынтығы. Екі актер қатысқанда, біреуі адам болуы керек, ал екіншісі адам немесе объект болуы мүмкін. Екіден көп қатысушы және бір немесе бірнеше өзара әрекеттесетін объектілер болған кезде топтық әрекет ым-ишараның, әрекеттердің немесе өзара әрекеттесудің комбинациясын қамтиды [22, 23].

Зорлық-зомбылықты анықтау. Зорлық-зомбылықты анықтау - әрекеттерді танудың кеңірек тақырыбы аясындағы бөлек мәселе. Зорлық-зомбылықты анықтаудың мақсаты - зорлық-зомбылықтың қысқа уақыт ішінде автоматты түрде және тиімді түрде орын алуын анықтау. Адам әрекеттерін автоматты түрде бейне анықтау соңғы жылдары бейнебақылау, адам мен компьютердің өзара әрекеттесуі және мазмұнға негізделген бейне іздеу сияқты қолданбалар үшін маңыздырақ болды [24].

Зорлық-зомбылықты анықтаудың мақсаты – зорлық – зомбылықтың автоматты түрде және тиімді түрде орын алуын анықтау болып табылады. Кез келген жағдайда зорлық-зомбылықты анықтаудың өзі қиын мәселе, өйткені зорлық-зомбылық түсінігі субъективті. Зорлық-зомбылықты анықтау оны

қарапайым әрекеттерден ерекшелендіретін ерекшеліктерге ие болғандықтан, ол қолданбалы деңгейде ғана емес, сонымен қатар зерттеу деңгейінде де күрделі мәселе болып табылады.

Зорлық-зомбылықты анықтау әдістерінің классификациясы

Күнделікті өмірде зорлық-зомбылық күдікті оқиғалар немесе әрекеттер ретінде анықталады. Бақылау камераларындағы мұндай әрекеттерді тану үшін компьютерлік көруді пайдалану әрекетті тану саласындағы танымал мәселеге айналды [25]. Ғалымдар зорлық-зомбылық немесе әдеттен тыс оқиғаларды анықтаудың әртүрлі тәсілдері мен әдістерін ұсынып, қылмыс деңгейінің тез өсуін тиімдірек анықтау қажеттілігінің мысалы ретінде көрсетті. Соңғы бірнеше жылда зорлық-зомбылықты анықтаудың әртүрлі әдістері жасалды. Қолданылған жіктеуіш негізінде зорлық-зомбылықты анықтау әдістері үш санатқа бөлінеді: машиналық оқыту арқылы зорлық-зомбылықты анықтау, SVM көмегімен зорлық-зомбылықты анықтау және терең оқыту арқылы зорлық-зомбылықты анықтау [26, 27]. SVM және терең оқыту компьютерлік көруде кеңінен қолданылатындықтан, олар дербес жіктеледі. Кестелер әрбір әдістің ерекшеліктерін түсіндіреді.

Машиналық оқыту әдістерін қолдану арқылы зорлық-зомбылықты анықтау. [28] Классикалық машиналық оқыту әдістерін қолданатын зорлық-зомбылықты анықтау әдістерін қарастырамыз. Сурет 1.2 – те бейне зорлық-зомбылықты анықтауға арналған әртүрлі жіктеу әдістерін жинақтаймыз, олар объектіні анықтауды, ерекшелікті алуды, жіктеуді, әдістердің әртүрлі көріністер түрлеріне қолданылуын және әртүрлі деректер жиындарында пайдаланылған кезде оларды бағалау параметрлерін көрсетілген.

| | | | | | | |
|--|---|--|---|---|----------------------------------|--|
| Serrano Gracia et al. (2015) | Motion blob acceleration measure vector method for detection of fast fighting from video | Ellipse detection method | An algorithm to find the acceleration | Spatio-temporal features use for classification | Both crowded and less crowded | Accuracy about 90% |
| Zhou et al. (2018) | FightNet for Violent Interaction Detection | Temporal Segment Network | Image acceleration | Softmax | Both crowded and uncrowded | 97% in Hockey, 100% in Movies dataset |
| Ribeiro, Audigier & Pham (2016) | RIMOC method focuses on speed and direction of an object on the base of HOF | Covariance Matrix method STV based | Spatio-temporal vector method (STV) | STV uses supervised learning | Both crowded and uncrowded | For normal situation 97% accuracy |
| Yao et al. (2021) | Multiview fight detection method | YOLO-V3 network | Optical flow | Random Forest | Both crowded and uncrowded | 97.66% accuracy 97.66 F1-score |
| Arceda et al. (2016) | Two step detection of violent and faces in video by using VIF descriptor and normalization algorithms | Vif object recognition CUDA method and KLT face detector | Horn shrunk method for histogram | Interpolation classification | Less crowded | Lower frame rate 14% too high rate of 35% fs/s 97% |
| Wu et al. (2020a), Wu et al. (2020b) | HL-Net to simultaneously capture long-range relations and local distance relations | HLC approximator | CNN based model | Weak supervision | Both crowded and uncrowded scene | 78.64% |
| Xie et al. (2016) | SVM method for recognition based on statistical theory frames | Vector normalization method | Macro block technique for features extractions | Region motion and descripton for video classification | Crowded | 96.1% accuracy |
| Febin, Jayasree & Joy (2020) | A cascaded method of violence detection based on MoBSIFT and movement filtering | MoBSIFT | Motion boundary histogram | SVM, random forest, and AdaBoost | Both Crowded and uncrowded scene | 90.2% accuracy in Hockey, 91% in Movies dataset |
| Senst et al. (2017) | Lagrangian fields of direction and begs of word framework to recognize the violence in videos | Global compensation of object motion | Lagrangian theory and STIP method for extract motion features | Late fusion for classification | Crowded | 91% to 94% accuracy |

Сурет 1.2 – Бейне зорлық-зомбылықты анықтауға арналған әртүрлі жіктеу әдістері

SVM көмегімен зорлық-зомбылықты анықтау әдістері. SVM негізіндегі зорлық-зомбылық оқиғасын тану әдістерінің жиынтығы сурет 1.3 – те

көрсетілген. SVM – жіктеу мәселелерін шешу үшін қолданылатын бақылаудағы оқыту әдісі. SVM компьютерлік көрудің танымал әдісі болып табылады, өйткені ол сенімді және сандық ақпаратты ескереді. Ол екілік жіктеу тапсырмаларын орындау үшін қолданылады.

| | | | | | |
|--|---|---|--|---|--|
| Ye et al. (2020) | A Video-Based DT-SVM School Violence Detecting Algorithm | Motion Co-occurrence Feature (MCF) | Optical flow extraction | Crowded | 97.6% |
| Zhang et al. (2016) | GMOF framework with tracking and detection module | Gaussian Mixture model | OHFO for optical flow extraction | Crowded | 82%-89% accuracy |
| Gao et al. (2016) | Violence detection using Oriented VIF | Optical Flow method | Combination of VIF and OVIF descriptor | Crowded | 90% |
| Deepak Vignesh & Chandrakala (2020) | Autocorrelation of gradients based violence detection | Motion boundary histograms | Frame based feature extraction | Crowded | 91.38% accuracy in Crowd Violence; 90.40% in Hockey dataset |
| Al-Navashi Al-Hazaimeh & Sarasa (2017) | Framework includes preprocessing, detection of activity and image retrieval. It identifies the abnormal event and image from data-based images. | Optical flow and tempora difference for object detection CBIR method for retrieving images. | Gaussian function for video future analysis | Less crowded | 97% accuracy |
| Kamouna et al. (2019) | Sparsity-Based Naive Bayes Approach for Anomaly Detection in Real Surveillance Videos | Sparsity-Based Naive Bayes | C3D feature extraction | Both crowded and uncrowded | 64.7% F1 score; 52.1% precision; 85.3% recall in UCF dataset |
| Song, Kim & Park (2018) | SGT-based and SVM-based multi-temporal framework to detect violent events in multi-camera surveillance. | Late fusion | Multi-temporal Analysis (MTA) | Variety fight scenes from minimum two to maximum fifteen people include various movements | 78.3% (SGT-based, BEHAVE), 70.2% (SVM-based, BEHAVE), 87.2% (SGT-based, NUS-HGA), and 69.9% (SGT-based, YouTube) |
| Yashitha, Bhatnagar & Khan (2018) | An architecture to identify violence in video surveillance system using VIF and LBP | Shape and motion analysis | VIF and Local Binary Pattern (LBP) descriptors | Both crowded and non-crowded scenes | 89.1% accuracy in Hockey dataset, 88.2% accuracy in Violent-Flow dataset |

Сурет 1.3 – SVM көмегімен зорлық-зомбылықты анықтау әдістері.

Терең оқыту арқылы зорлық-зомбылықты анықтау әдістері. Графикалық ресурстарда зорлық-зомбылықты анықтауда терең оқыту алгоритмдерін қолдану бағытындағы зерттеу жұмыстары күннен күнге жақсарып келеді. Конволюциялық нейрондық желілер (CNNs) және олардың жақсартулары бейнелердегі зорлық-зомбылықты анықтау үшін кеңінен қолданылады. Сурет 1.4-те терең оқытуға негізделген тану әдістерінің жинағы көрсетілген. Нейрондық желілер терең оқытудың негізі болып табылады. Қосымша конволюционды қабаттарды пайдалана отырып, әдіс деректер жинағы мен алынған мүмкіндіктер негізінде мәжбүрлі тануды жіктеу үшін қолданылады.

| | | | | | |
|---|---|---|---|-----------------------------------|--|
| Ding et al. (2014) | Violence Detection using 3D CNN | 3D convolution is used to get spatial information | Backpropagation method | Crowded | 91% accuracy |
| Arandjelovic et al. (2016) | Deep architecture for place recognition | VGG VLAD method for image retrieval | Backpropagation method for feature extraction | Crowded | 87%-96% accuracy |
| Fenil et al. (2019) | Framework for football stadium comprising of big data analysis and deep learning through bidirectional LSTM | Bidirectional LSTM | HOG, SVM | Crowded | 94.5% accuracy |
| Mu, Cao & Jin (2016) | Violent scene detection using CNN and deep audio features | MFB | CNN | Crowded | Approximately 90% accuracy |
| Mohitavipour, Saiedi & Arabsoorkhi (2021) | A multi-stream CNN using handcrafted features | A deep violence detection framework based on the specific features (speed of vmovement, and representative image) derived from handcrafted methods. | CNN | Both crowded and uncrowded | |
| Sudhakaran & Lanz (2017) | Detect violent videos using ConvLSTM | CNN along with the ConvLSTM | CNN | Crowded | Approximately 97% |
| Naik & Gopalakrishna (2021) | Deep violence detection framework based on the specific features derived from handcrafted methods | Discriminative feature with a novel differential motion energy image | CNN | Both crowded and uncrowded | |
| Meng, Yuan & Li (2017) | Detecting Human Violent Behavior by integrating trajectory and Deep CNN | Deep CNN | Optical flow method | Crowded | 98% accuracy |
| Rendón-Segador et al. (2021) | ViolenceNet: Dense Multi-Head Self-Attention with Bidirectional Convolutional LSTM | 3D DenseNet | Optical flow method | Crowded | 95.6%- 100% accuracy |
| Xia et al. (2018) | Violence detection method based on a bi-channels CNN and the SVM. | Linear SVM | Bi-channels CNN | Both crowded and uncrowded scenes | 95.90 ± 3.53 accuracy in Hockey fight, 93.25 ± 2.34 accuracy in Violence crowd |
| Meng et al. (2020) | Trajectory-Pooled Deep Convolutional Networks | ComNet model which contains 17 convolutionpool-norm | Deep ConvNet model | Both crowded and | 92.5% accuracy in Crowd Violence, 98.6% in |

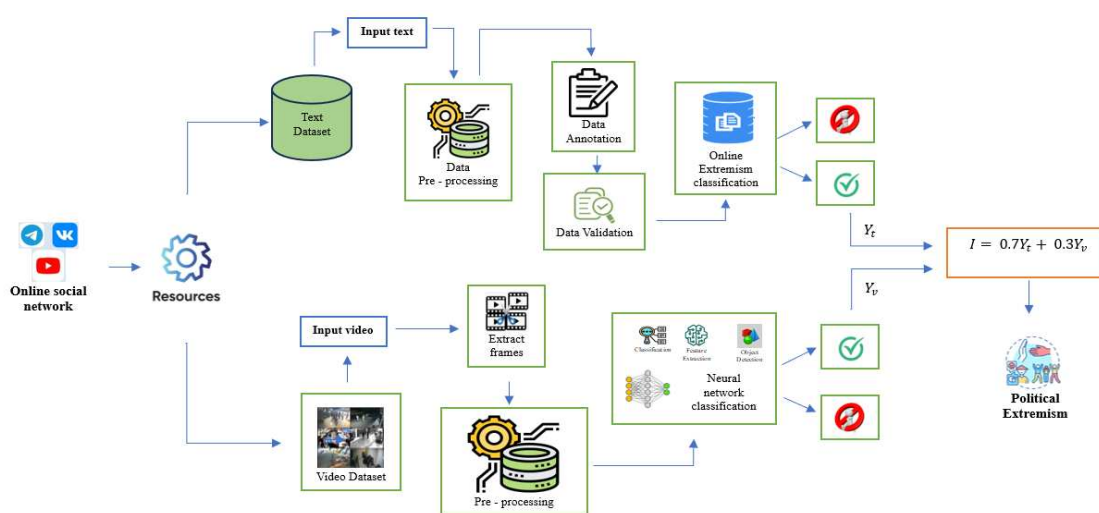
Сурет 1.4 – Терең оқыту әдістерін қолдану арқылы зорлық-зомбылықты анықтау.

1.4 Онлайн әлеуметтік желілерді саяси экстремистік мәтіндер мен графикалық ресурстарды анықтаудағы есептің қойылымы

Әлемде болып жатқан соңғы өзгерістер өмірдің барлық салаларына әсер ететіні сөзсіз. Халқымызды жағымсыз жаңалықтарға, зорлық – зомбылыққа толы бейнелерге, лаңкестік идеяларға толы әлеуметтік желілерде тарайтын контенттерден сақтап қалу, күннен күнге қиындап барады. Сонымен қатар, әлеуметтік желілерде көптеген кәсіби манипуляторлар жұмыс істейді, оларға жарнама берушілер, үгітшілер, саяси стратегтер, экстремистер мен қылмыскерлер, деструктивті топтарды ұйымдастырушыларды жатқызуға болады. Әлеуметтік медиа кеңістігі – жарнама, санаға әсер ету, қылмысқа, үгіт-насихатқа, ақпараттық соғысқа, экстремизмді насихаттауға және тәртіпсіздіктерді ұйымдастыруға арналған тамаша құрал.

Дәл әлеуметтік желілер бүгінгі күні деструктивті идеологиялар мен құбылыстарды таратудың негізгі арнасына айналды:

- 1) кибербуллинг (қудалау), троллинг;
- 2) экстремизм және терроризм;
- 3) саясиландырылған деструктивті қозғалыстар;
- 4) нашақорлық, педофилия және жыныстық азғындық;
- 5) қауіпті ойындар мен «чалленджер»;
- 6) қауіпті субмәдениеттер (мектеп атқыштары, маньяктар мен өлтірушілер культі);
- 7) сананы манипуляциялау;
- 8) шок мазмұны және т.б.



Сурет 1.5 – Саяси экстремизмді анықтау әдістемесінің жалпы үлгісі

Осы аталғандардың барлығы дерлік қауіпті, соның ішінде экстремистік контенттерден зиян шегушілер саны жыл сайын артып келеді. Интернеттегі экстремизмнің алдын алу саласындағы құзыреттерді жетілдіру

технологияларына зерттеу жүргізу барысында, онлайн әлеуметтік желілердінде саяси экстремисттік мәтіндер мен графикалық ресурстарды анықтауға арналған бағдарламалық жабдықтаманы әзірлеу идеясы туындаған болатын. Сол орайда ұзақ зерттеулер жүргізіліп, әлемдік деңгейдегі бағдарламалық жүйелерге шолу жасалып, әртүрлі модельдер мен әдістер қолданылды. Әлеуметтік желілердегі контенттер бірнеше сипатта болатындықтан, мәтіндік және графикалық ресурстардан саяси экстремизм мазмұнын анықтаудың дәлдігін арттыру мақсаты қойылды.

Саяси экстремизмді анықтау әдістемесінің жалпы үлгісіне тоқталатын болсақ, алдымен әлеуметтік желілерде жарияланған посттардан мәтіндік және графикалық ресурстар алынып, бірнеше процестерден өткізіледі, содан соң интегралды бағалау шартына сәйкес алынған ресурстарда саяси экстремисттік мазмұн бар – жоғы анықталады. Келесі таралауларда әзірленген бағдарламалық жасақтаманың барлық кезеңдеріне нақты сипаттама беріледі.

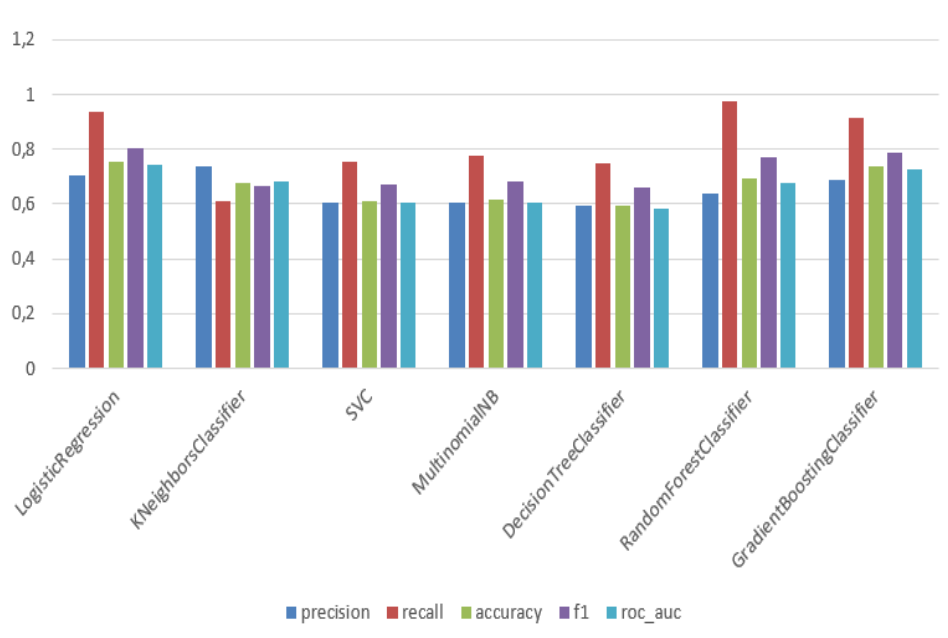
2 ӘЛЕУМЕТТІК ЖЕЛІЛЕРІНДЕ САЯСИ ЭКСТРЕМИЗМДІ АНЫҚТАУ ПРОЦЕСТЕРІН МОДЕЛЬДЕУ

2.1 Саяси экстремисттік мәтіндік контентті анықтау модельдерінің классификациясы

Жинақталған мәтіндерден белгілерді өңдеу. Бұл бөлімде біз саяси экстремизмді әртүрлі белгілердің комбинацияларын қолдана отырып жіктеу үшін әртүрлі Машиналық оқыту модельдері мен әдістерін қолдану нәтижелерін салыстырамыз.

Қазіргі заманғы зерттеулер жіктеуіштерді құру мен оқытудың келесі кең таралған әдістерін қарастырады: LogisticRegression (логистикалық регрессия), KNeighborsClassifier (k-жақын көршілер), SVC (тірек векторлық машина), MultinomialNB (аңғал Байес), DecisionTreeClassifier (шешім ағашы), RandomForestClassifier (кездейсоқ орман), GradientBoostingClassifier (Градиентті күшейту).

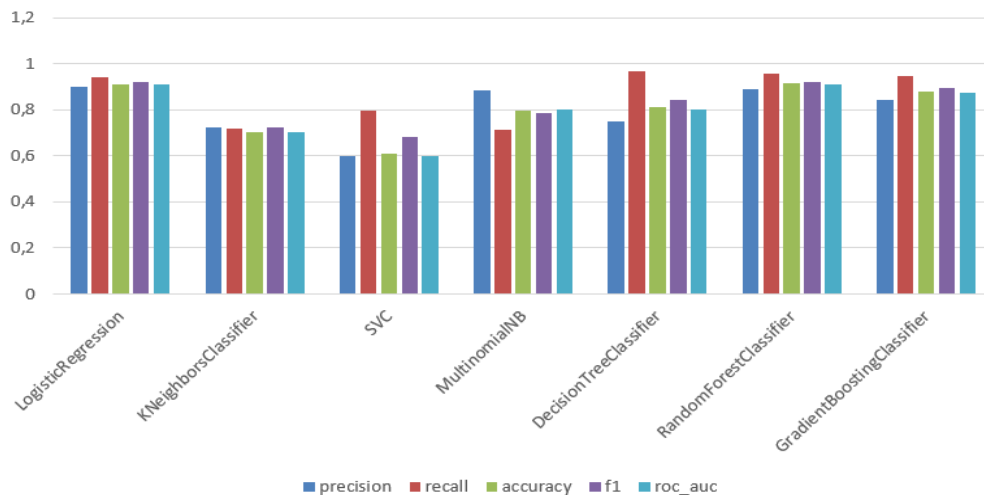
Word2Vec (WordToVectorizer – сөзден векторға) сөздерді векторларға түрлендіру, осылайша олардың мағынасын, семантикалық ұқсастығын және қоршаған мәтінмен байланысын анықтау үшін қолданылатын әдіс. Бұл әдіс компьютерлерге жаңалықтар мақалалары мен кітаптар сияқты үлкен мәтіндік жинақтардағы өрнектер мен кілт сөздердің контекстін және мағынасын білуге көмектеседі [29].



Сурет 2.1 – Жіктеу алгоритмдерінің нәтижелерін салыстыру (Word2Vec)

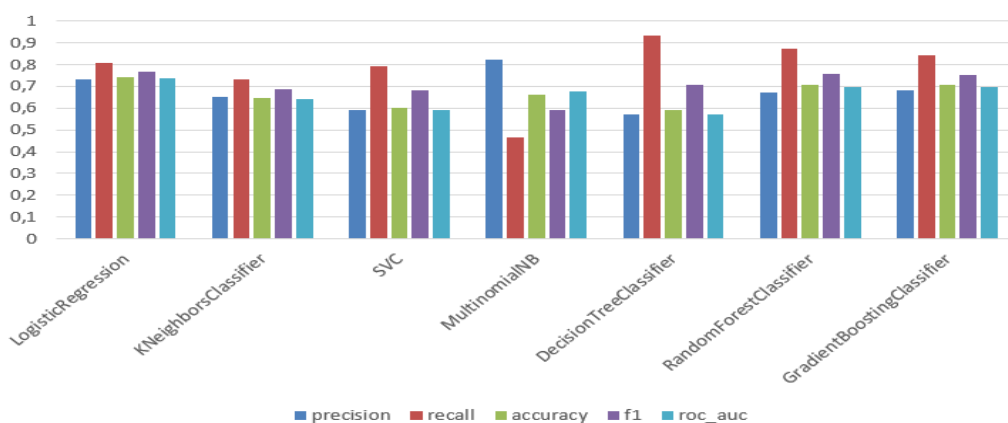
Word2Vec (сурет 2.1) негізгі идеясы әрбір сөзді жоғары өлшемді вектор ретінде көрсету болып табылады, мұнда вектордың осы жоғары өлшемді кеңістіктегі орны сөздің мағынасын көрсетеді.

Word2Vec — мәтіндердің үлкен корпусынан сөздердің мағынасын білу үшін ұсақ түйіршікті нейрондық желі моделін пайдаланатын алгоритм. Бірнеше жасырын қабаттары бар терең нейрондық желілерден (DNN) айырмашылығы, таяз нейрондық желілерде кіріс пен шығыс арасында тек бір немесе екі жасырын қабат болады.



Сурет 2.2 – Жіктеу алгоритмдерінің нәтижелерін салыстыру (TF-IDF Vectorizer (bigram))

TF-IDF мәтіндік деректерден мүмкіндіктерді алудың ең кең таралған және күшті әдістерінің бірі болып табылады. TF-IDF құжаттағы әрбір сөздің маңыздылығын оның құжатта және мәтіндердің бүкіл жинағында пайда болу санына қатысты есептейді. Бұл әдіс кілт сөздерді бөлектеуге және бүкіл жинақ контекстінде белгілі бір құжат үшін қандай сөздердің көбірек салмақ түсіретінін түсінуге мүмкіндік береді.



Сурет 2.3 – Жіктеу алгоритмдерінің нәтижелерін салыстыру (TF-IDF Vectorizer)

TF-IDF негіздері, TF-IDF түсінігі және формуласы

"TF" (Термдік жиілік) және "IDF" (кері құжат жиілігі) терминдері

TF (Терм. жиілігі) белгілі бір сөздің берілген құжатта қаншалықты жиі кездесетінін білдіреді. Осылайша, TF жеке құжат контекстінде сөздің маңыздылығын өлшейді.

IDF (кері құжат жиілігі) құжаттың бүкіл жинағында сөздің қаншалықты бірегей екенін өлшейді. Құжаттардың көпшілігінде кездесетін сөздердің IDF деңгейі төмен, себебі олар көп ақпарат мәнін бермейді.

Жоғарыда көрсетілген графиктерге сәйкес Word2Vec, TF-IDF, TF-IDFbigram алгоритмдерінің нәтижесінде өңделмеген мәтіндерде Логистикалық регрессия (Logistic Regression) әдісі ең жоғары AUC 0,9235 ие, ал ең төменгі көрсеткіш тірек векторлық машинаса әдісінде. AUC мәні шамамен AUC мәні 0,5917 тең.

Мәтінді алдын ала өңдеуден кейінгі нәтижелер

Кесте 2.1–де әртүрлі белгілерді қолдана отырып, әртүрлі әдістерді салыстыру нәтижелерін көрсетеді. Кестеде көрсетілгендей, барлық әдістердің өнімділігі тұтастай алғанда көбірек функцияларды біріктіру арқылы жақсарады. Бұл бақылау алынған белгілердің ақпараттылығы мен тиімділігін растайды. Дегенмен, әрбір белгінің үлесі айтарлықтай өзгереді, бұл жеке әдістердің нәтижелерінің ауытқуын көрсетеді.

Кесте 2.1 – Әр түрлі белгілерді қолдана отырып, әртүрлі әдістерді салыстыру

| Ерекшеліктері | Әдістер | Prec. | recall | Accur. | f1 | roc_auc |
|--|----------------------------|--------|--------|--------|--------|---------|
| Word2Vec (dataset+spellchecker) | LogisticRegression | 0,8483 | 0,8174 | 0,8182 | 0,8326 | 0,8183 |
| | KNeighborsClassifier | 0,7683 | 0,6963 | 0,7159 | 0,7305 | 0,7182 |
| | SVC | 0,6550 | 0,7717 | 0,6490 | 0,7086 | 0,6344 |
| | MultinomialNB | 0,6468 | 0,7945 | 0,6465 | 0,7131 | 0,6289 |
| | DecisionTreeClassifier | 0,6263 | 0,8151 | 0,6288 | 0,7083 | 0,6067 |
| | RandomForestClassifier | 0,7339 | 0,9384 | 0,7778 | 0,8236 | 0,7587 |
| | GradientBoostingClassifier | 0,7751 | 0,8813 | 0,7929 | 0,8248 | 0,7824 |
| TF-IDF Vectorizer (bigram) (dataset+spellchecker) | LogisticRegression | 0,9213 | 0,9361 | 0,9205 | 0,9287 | 0,9186 |
| | KNeighborsClassifier | 0,7460 | 0,7511 | 0,7210 | 0,7486 | 0,7174 |
| | SVC | 0,6314 | 0,7352 | 0,6162 | 0,6793 | 0,6020 |
| | MultinomialNB | 0,8947 | 0,7763 | 0,8258 | 0,8313 | 0,8316 |
| | DecisionTreeClassifier | 0,7839 | 0,9772 | 0,8384 | 0,8699 | 0,8219 |
| | RandomForestClassifier | 0,9121 | 0,9475 | 0,9205 | 0,9295 | 0,9172 |
| | GradientBoostingClassifier | 0,8987 | 0,9726 | 0,9242 | 0,9342 | 0,9185 |
| TF-IDF Vectorizer (dataset+spellchecker) | LogisticRegression | 0,7740 | 0,8288 | 0,7715 | 0,8004 | 0,7647 |
| | KNeighborsClassifier | 0,7171 | 0,7580 | 0,7008 | 0,7370 | 0,6940 |
| | SVC | 0,6191 | 0,7831 | 0,6136 | 0,6915 | 0,5935 |
| | MultinomialNB | 0,8672 | 0,5068 | 0,6843 | 0,6398 | 0,7054 |
| | DecisionTreeClassifier | 0,6743 | 0,6712 | 0,6389 | 0,6728 | 0,6351 |
| | RandomForestClassifier | 0,7054 | 0,9018 | 0,7374 | 0,7916 | 0,7179 |
| | GradientBoostingClassifier | 0,7164 | 0,8767 | 0,7399 | 0,7885 | 0,7237 |

Кесте 2.1 – жалғасы

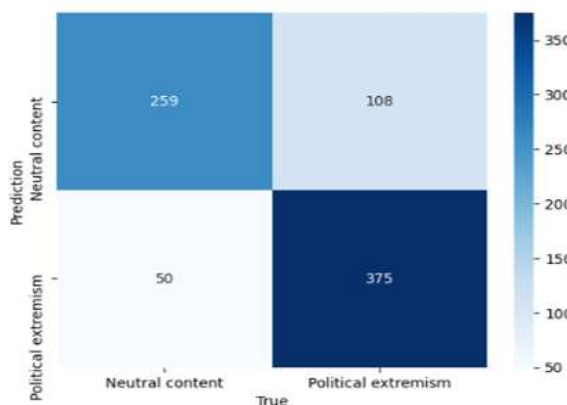
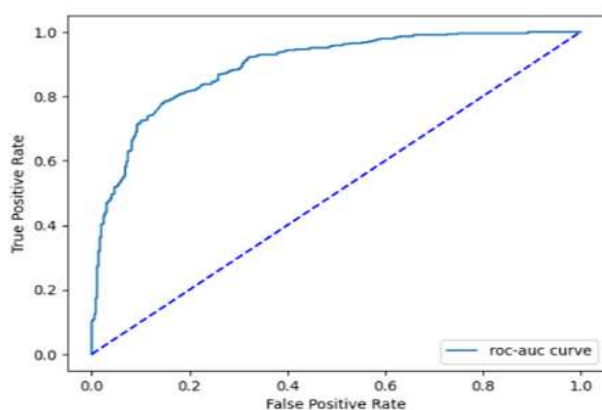
| | | | | | | |
|---|----------------------------|--------|--------|--------|--------|--------|
| Word2Vec (main dataset+stemming) | LogisticRegression | 0,8883 | 0,6989 | 0,7765 | 0,7823 | 0,7901 |
| | KNeighborsClassifier | 0,7880 | 0,7187 | 0,7273 | 0,7517 | 0,7288 |
| | SVC | 0,6654 | 0,7824 | 0,6490 | 0,7192 | 0,6256 |
| | MultinomialNB | 0,6764 | 0,8176 | 0,6705 | 0,7403 | 0,6447 |
| | DecisionTreeClassifier | 0,7807 | 0,7121 | 0,7197 | 0,7448 | 0,7210 |
| | RandomForestClassifier | 0,8031 | 0,9143 | 0,8220 | 0,8551 | 0,8058 |
| | GradientBoostingClassifier | 0,8330 | 0,8659 | 0,8232 | 0,8491 | 0,8158 |
| TF-IDF Vectorizer (bigram) (main dataset+stemming) | LogisticRegression | 0,9237 | 0,9582 | 0,9306 | 0,9407 | 0,9257 |
| | KNeighborsClassifier | 0,7640 | 0,8110 | 0,7475 | 0,7868 | 0,7364 |
| | SVC | 0,6583 | 0,8088 | 0,6490 | 0,7258 | 0,6210 |
| | MultinomialNB | 0,9407 | 0,8022 | 0,8573 | 0,8660 | 0,8670 |
| | DecisionTreeClassifier | 0,7831 | 1,0000 | 0,8409 | 0,8784 | 0,8131 |
| | RandomForestClassifier | 0,9158 | 0,9560 | 0,9242 | 0,9355 | 0,9187 |
| | GradientBoostingClassifier | 0,8975 | 0,9626 | 0,9154 | 0,9290 | 0,9071 |
| TF-IDF Vectorizer (main dataset+stemming) | LogisticRegression | 0,7856 | 0,8857 | 0,7955 | 0,8326 | 0,7797 |
| | KNeighborsClassifier | 0,7192 | 0,8330 | 0,7172 | 0,7719 | 0,6969 |
| | SVC | 0,6486 | 0,7868 | 0,6326 | 0,7110 | 0,6056 |
| | MultinomialNB | 0,9246 | 0,5121 | 0,6957 | 0,6591 | 0,7279 |
| | DecisionTreeClassifier | 0,6584 | 0,8725 | 0,6667 | 0,7505 | 0,6306 |
| | RandomForestClassifier | 0,7597 | 0,9033 | 0,7803 | 0,8253 | 0,7588 |
| | GradientBoostingClassifier | 0,7547 | 0,8857 | 0,7689 | 0,8150 | 0,7485 |
| Word2Vec (dataset+spellchecker+stemming) | LogisticRegression | 0,8219 | 0,8471 | 0,8194 | 0,8343 | 0,8173 |
| | KNeighborsClassifier | 0,7662 | 0,7247 | 0,7336 | 0,7449 | 0,7343 |
| | SVC | 0,6308 | 0,7318 | 0,6263 | 0,6776 | 0,6179 |
| | MultinomialNB | 0,6387 | 0,8071 | 0,6515 | 0,7131 | 0,6392 |
| | DecisionTreeClassifier | 0,6720 | 0,5929 | 0,6263 | 0,6300 | 0,6289 |
| | RandomForestClassifier | 0,7616 | 0,9624 | 0,8182 | 0,8503 | 0,8068 |
| | GradientBoostingClassifier | 0,7749 | 0,9153 | 0,8119 | 0,8393 | 0,8037 |
| TF-IDF Vectorizer (bigram) (dataset+spellchecker+stemming) | LogisticRegression | 0,9063 | 0,9553 | 0,9230 | 0,9301 | 0,9204 |
| | KNeighborsClassifier | 0,7473 | 0,8141 | 0,7525 | 0,7793 | 0,7477 |
| | SVC | 0,6257 | 0,7788 | 0,6313 | 0,6939 | 0,6197 |
| | MultinomialNB | 0,8998 | 0,8659 | 0,8763 | 0,8825 | 0,8771 |
| | DecisionTreeClassifier | 0,7733 | 0,9953 | 0,8409 | 0,8704 | 0,8287 |
| | RandomForestClassifier | 0,9213 | 0,9647 | 0,9369 | 0,9425 | 0,9347 |
| | GradientBoostingClassifier | 0,9252 | 0,9600 | 0,9369 | 0,9423 | 0,9350 |
| TF-IDF Vectorizer (dataset+spellchecker+stemming) | LogisticRegression | 0,7764 | 0,8824 | 0,8005 | 0,8260 | 0,7940 |
| | KNeighborsClassifier | 0,6978 | 0,8259 | 0,7146 | 0,7565 | 0,7059 |
| | SVC | 0,6166 | 0,8400 | 0,6338 | 0,7112 | 0,6175 |
| | MultinomialNB | 0,8860 | 0,5671 | 0,7285 | 0,6915 | 0,7413 |
| | DecisionTreeClassifier | 0,6152 | 0,9553 | 0,6553 | 0,7484 | 0,6316 |
| | RandomForestClassifier | 0,7398 | 0,9365 | 0,7891 | 0,8266 | 0,7775 |
| | GradientBoostingClassifier | 0,7379 | 0,8941 | 0,7727 | 0,8085 | 0,7631 |

Кесте 2.1 – сәйкес Логистикалық регрессия (LogisticRegression) әдісі ең жоғары AUC 0,7940 ие, ал ең төменгі көрсеткіш тірек векторлық машинаса әдісінде. AUC мәні шамамен AUC мәні 0,6175 тең.

Әдістерге салыстырмалы талдау (TF-IDF биграммалар арқылы құрылған векторизатор).

Логистикалық регрессия (LogisticRegression).

Логистикалық регрессия – категориялық тәуелді айнымалының ықтималдығын болжау үшін қолданылатын машиналық оқытуды жіктеу алгоритмі. Логистикалық регрессияда тәуелді айнымалы 1 (иә, сәтті және т.б.) немесе 0 (жоқ, сәтсіздік және т.б.) ретінде кодталған деректерді қамтитын екілік айнымалы болып табылады. Басқаша айтқанда, логистикалық регрессия моделі $P(Y=1) X$ функциясы ретінде болжайды [30].



Сурет 2.4 – Логистикалық регрессия әдісі арқылы жіктеудің дәлсіздік матрицасы мен ROC қисық түріндегі нәтижесі

Логистикалық регрессиялық жорамалдар:

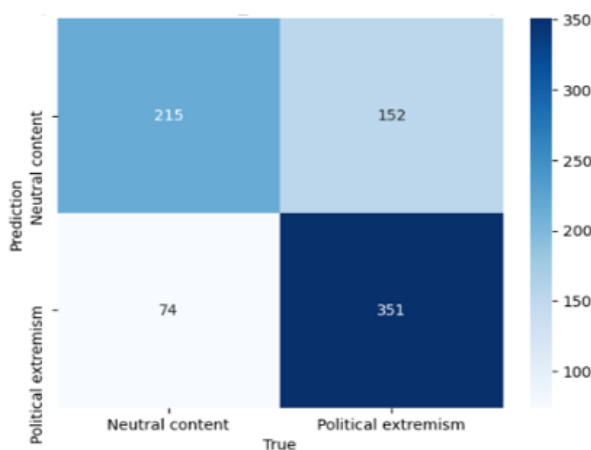
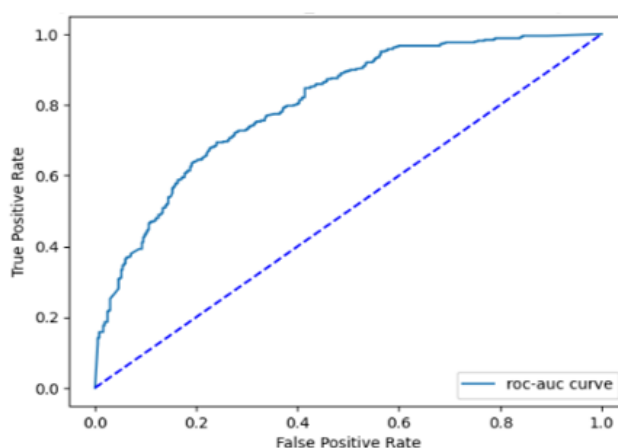
- Екілік логистикалық регрессия тәуелді айнымалының екілік болуын талап етеді;
- Екілік регрессия үшін тәуелді айнымалының 1-фактор деңгейі қажетті нәтижені көрсетуі керек;
- Тек маңызды айнымалыларды қосу керек;

- Тәуелсіз айнымалылар бір-бірінен тәуелсіз болуы керек. Яғни, модельде мультиколлинеарлық аз немесе мүлдем болмауы керек;
- Тәуелсіз айнымалылар журнал коэффициенттерімен сызықты түрде байланысты.

- Логистикалық регрессия үлкен үлгі өлшемдерін талап етеді.

k-жақын көршілер (KNeighborsClassifier).

k-жақын көршілер – бақыланатын оқыту әдісіне негізделген машиналық оқытудың ең қарапайым алгоритмдерінің бірі. Жаңа жағдай/деректер мен қолжетімді бақылаулар арасындағы ұқсастықты болжайды және жаңа жағдайды қолжетімді санаттарға барынша ұқсас санатқа орналастырады. K-NN алгоритмі барлық қолжетімді деректерді сақтайды және ұқсастық негізінде жаңа деректер нүктесін жіктейді.



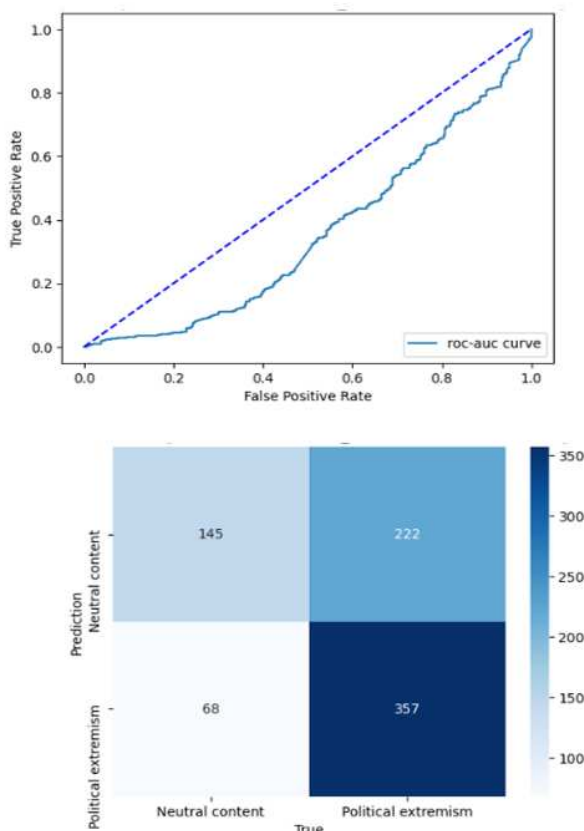
Сурет 2.5 – K-жақын көршілер әдісі арқылы жіктеудің дәлсіздік матрицасы мен ROC қисық түріндегі нәтижесі

Бұл жаңа деректер қол жетімді болғанда, оны K-NN алгоритмі арқылы ұңғыма ретінде оңай жіктеуге болатынын білдіреді. Бұл алгоритмді регрессия үшін де, жіктеу үшін де қолдануға болады, бірақ ол негізінен жіктеу есептері үшін қолданылады. Параметрлік емес алгоритм болып табылады, яғни ол негізгі

деректер туралы ешқандай жорамал жасамайды. Ол оқыту жиынынан бірден үйренбей, деректер жиынын сақтайтындықтан және жіктеу кезінде деректер жиынында әрекетті орындайтындықтан, оны жалқау оқыту алгоритмі деп те атайды. KNN алгоритмі өзінің оқыту кезеңінде жай ғана деректер жинағын сақтайды және ол жаңа деректерді алған кезде бұл деректерді жаңа деректерге өте ұқсас категорияға жіктейді.

Тірек векторлық машина (SVC).

Тірек векторлық машинасы немесе SVM классификация мен регрессия мәселелерін шешу үшін қолданылатын ең танымал бақыланатын оқыту алгоритмдерінің бірі болып табылады. Дегенмен, ол негізінен машиналық оқытудағы жіктеу мәселелері үшін қолданылады.

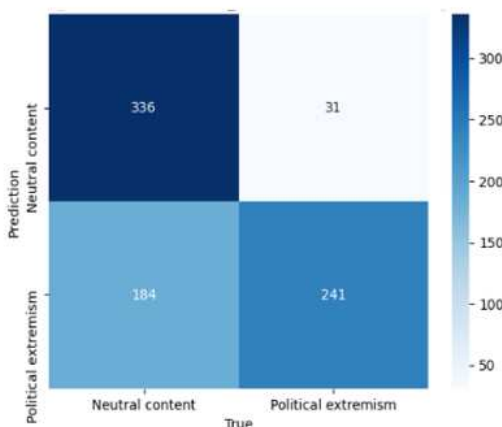
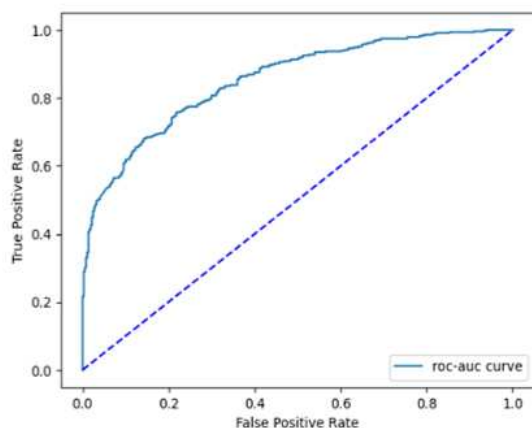


Сурет 2.6 – Тірек векторлық машина әдісі арқылы жіктеудің дәлсіздік матрицасы мен ROC қисық түріндегі нәтижесі

SVM алгоритмінің мақсаты болашақта жаңа деректер нүктесін дұрыс санатқа оңай орналастыру үшін n өлшемді кеңістікті сыныптарға бөле алатын ең жақсы сызық немесе шешім шекарасын жасау болып табылады. Ең жақсы шешімнің бұл шекарасы гипержазықтық деп аталады. SVM гипержазықтықты жасауға көмектесетін экстремалды нүктелерді/векторларды таңдайды. Бұл экстремалды жағдайлар тірек векторлық машиналар деп аталады, сондықтан алгоритм тірек векторлық машина деп аталады.

Аңғал Байес (MultinomialNB)

Аңғал Байес – табиғи тілді өңдеуде (NLP) мәтінді жіктеу мәселелерін шешуге арналған танымал машиналық оқыту алгоритмі. Бұл әсіресе сөз жиілігін санау сияқты дискретті сипаттамалары бар мәтіндік деректерді қамтитын тапсырмалар үшін пайдалы. MNB Байес теоремасының принципі бойынша жұмыс істейді және класс айнымалысын ескере отырып, мүмкіндіктер шартты түрде тәуелсіз деп есептейді.



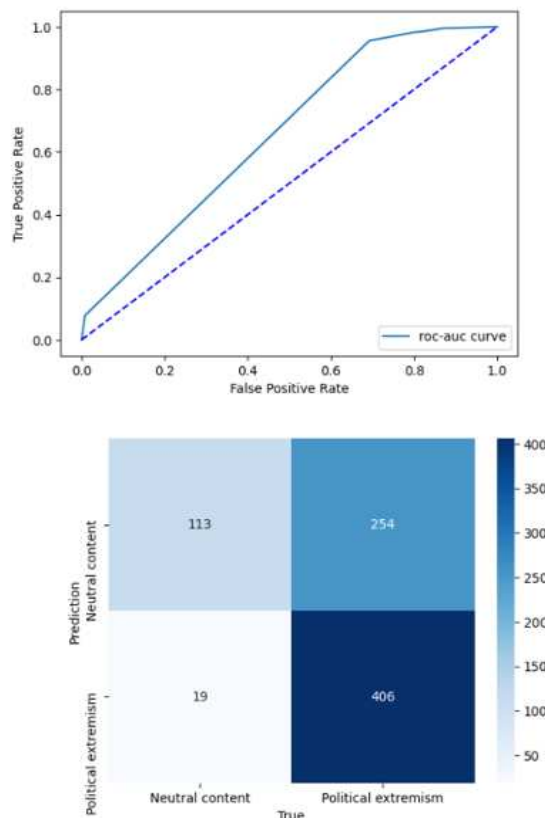
Сурет 2.7 – Аңғал Байес әдісі арқылы жіктеудің дәлсіздік матрицасы мен ROC қисық түріндегі нәтижесі

Naive Bayes классификаторының алгоритмі - бұл әр жұп белгілер арасындағы шартты тәуелсіздіктің «аңғал» жорамалымен Байес теоремасын қолдануға негізделген ықтималдық алгоритмдер тобы. Бэйс теоремасы $P(c|x)$ ықтималдығын есептейді, мұндағы c - мүмкін болатын нәтижелер класы, ал x - кейбір ерекше белгілерді білдіретін жіктелетін берілген данасы.

Шешім ағашы (DecisionTreeClassifier).

Шешім ағашы– регрессия мен жіктеу тапсырмаларын орындау мүмкіндігі бар, бақыланатын пайдалы машиналық оқыту алгоритмдері. Ол түйіндер мен тармақтармен сипатталады, мұнда әрбір атрибут бойынша сынақтар түйіндерде көрсетіледі, осы процедураның нәтижесі тармақтарда және класс белгілері

жапырақ түйіндерінде (листовых узлах) көрсетіледі. Сондықтан ол ықтимал нәтижелерін есептеу үшін қолданылатын әртүрлі шешімдерге негізделген ағаш тәрізді модельді пайдаланады. Ағаш негізіндегі алгоритмдердің бұл түрлері, бұл алгоритмдерді түсіндіру және пайдалану оңай болғандықтан, ең көп қолданылатын алгоритмдердің бірі болып табылады. Бұдан басқа, осы алгоритм әзірлеген болжамды модельдер жақсы тұрақтылық пен түсіру дәлдігіне ие, сондықтан олар өте танымал.



Сурет 2.8 – Шешім ағашы әдісі арқылы жіктеудің дәлсіздік матрицасы мен ROC қисық түріндегі нәтижесі

Шешім ағаштарының артықшылықтары:

- Түсінуге және түсіндіруге оңай;
- Деректерді қалыпқа келтіруді қажет етпейді;
- Деректерді масштабтау қажеттілігін жеңілдетпейді;
- Алдын ала өңдеу қадамы басқа негізгі алгоритмдермен салыстырғанда аз күш жұмсауды қажет етеді, демек, белгілі бір мағынада берілген тапсырманы оңтайландырады.

Шешім ағаштарының кемшіліктері:

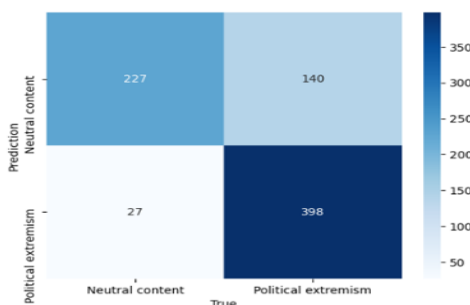
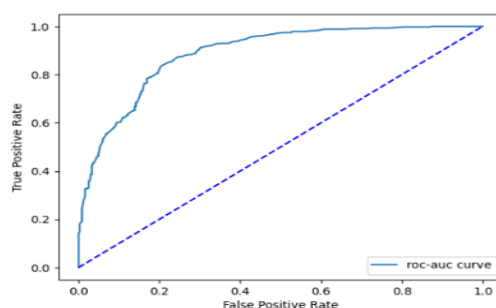
- Модельді үйрету үшін көбірек уақыт қажет;
- Оның айтарлықтай күрделілігі бар және деректерді өңдеу үшін көбірек уақыт қажет;

- Пайдаланушы енгізу параметрінің төмендеуі өте аз болғанда, бұл ағаштың аяқталуына әкеледі;

- Есептеулер кейде өте күрделі болуы мүмкін.

Кездейсоқ орман (RandomForestClassifier)

Кездейсоқ орман дәлірек болжам жасау үшін бірнеше шешім ағаштарын құрастырады және біріктіреді. Бұл сызықтық емес жіктеу алгоритмі. Әрбір шешім ағашының үлгісі бөлек пайдаланылады. Ағашты құрастыру кезінде пайдаланылмайтын жағдайлардың қателігінің бағасы жасалды. Бұл пайызбен берілген қапшықтан тыс қателік бағалау деп аталады. Олар кездейсоқ деп аталады, өйткені олар оқыту кезінде кездейсоқ болжауыштарды таңдайды. Олар орман ағаштары деп аталады, өйткені олар шешім қабылдау үшін бірнеше ағаштардың нәтижелерін пайдаланады. Кездейсоқ орман шешім ағаштарынан жоғарырақ, себебі жұмыс істейтін көптеген байланыссыз ағаштар (модельдер) әрқашан модельдің жеке құрамдас бөліктерінен асып түседі.



Сурет 2.9 – Кездейсоқ орман әдісі арқылы жіктеудің дәлсіздік матрицасы мен ROC қисық түріндегі нәтижесі

Random Forest байқаулардың кездейсоқ үлгілерін, кездейсоқ бастапқы айнымалыларды (бағандарды) алады және модель құру әрекетін жасайды.

Кездейсоқ орманның артықшылықтары:

- Кездейсоқ орман классификация және регрессия тапсырмаларын орындауға қабілетті;

- Ол жоғары өлшемділігі бар үлкен деректер жиынын өңдеуге қабілетті;

- Бұл модельдің дәлдігін арттырады және артық орнату мәселесін болдырмайды.

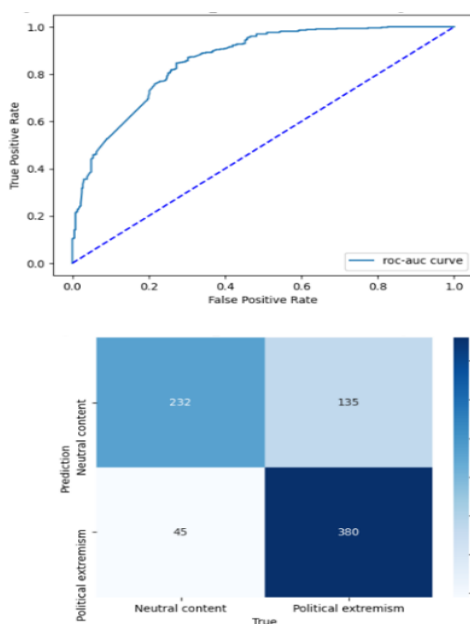
Кездейсоқ орманның кемшіліктері:

- Кездейсоқ орман жіктеу және регрессия тапсырмалары үшін де пайдаланылуы мүмкін болса да, ол Регрессия тапсырмалары үшін қолайлы емес.

Градиентті күшейту (GradientBoostingClassifier)

Градиентті күшейту – классификация және регрессия мәселелері үшін қолданылатын машиналық оқытудағы танымал күшейту алгоритмі. Күшейту - бұл әрбір жаңа үлгі алдыңғы үлгіні түзетуге әрекеттенетін модельді дәйекті түрде жаттықтыратын ансамбльді оқыту әдісінің түрі. Ол бірнеше әлсіз оқушыларды мықты студенттерге біріктіреді. Ең танымал екі күшейту алгоритмі бар, олар:

- AdaBoost
- Градиентті күшейту



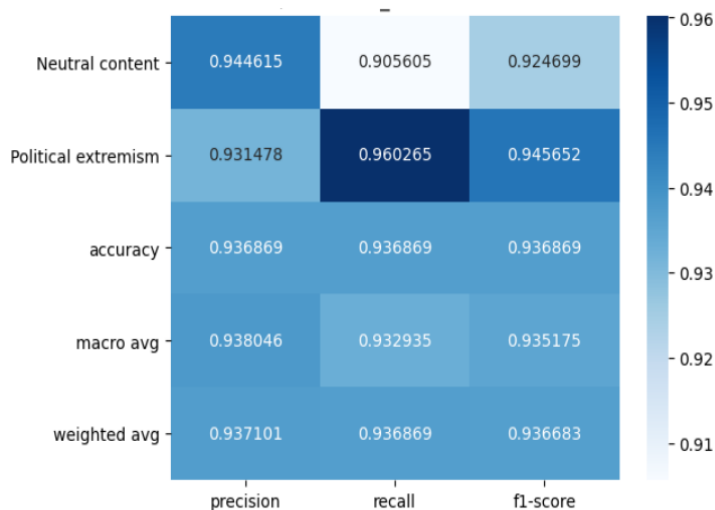
Сурет 2.10 – Градиентті күшейту әдісі арқылы жіктеудің дәлсіздік матрицасы мен ROC қисық түріндегі нәтижесі

Gradient Boosting – бірнеше әлсіз оқушыларды күшті оқушыларға біріктіретін қуатты күшейту алгоритмі, онда әрбір жаңа модель градиенттің түсуін пайдалана отырып, алдыңғы үлгідегі орташа квадраттық қате немесе кросс энтропия сияқты жоғалту функциясын азайтуға үйретіледі. Әрбір итерацияда алгоритм ағымдағы ансамбльдің болжамдарына қатысты жоғалту функциясының градиентін есептейді, содан кейін осы градиентті азайту үшін жаңа әлсіз үлгіні жаттықтырады. Содан кейін жаңа үлгінің болжамдары ансамбльге қосылады және тоқтату критерийі орындалғанша процесс қайталанатын.

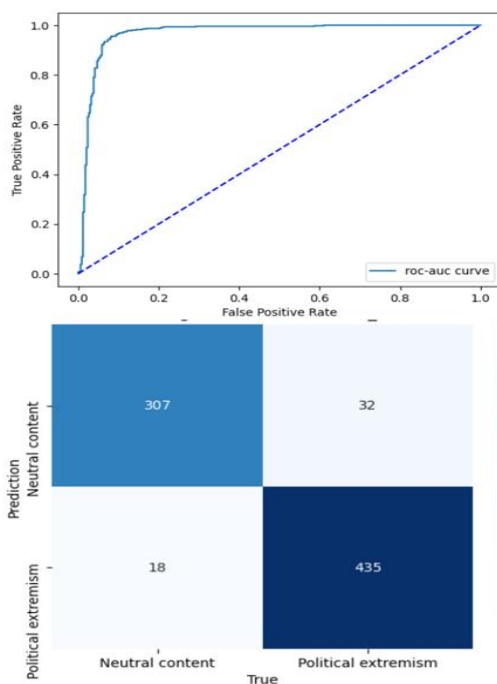
AdaBoost-тен айырмашылығы, оқыту даналарының салмақтары реттелмейді, оның орнына әрбір болжаушы белгі ретінде алдыңғы нұсқаның қалдық қателерін пайдалана отырып оқытылады.

POLIT_LSTM әдісі

POLIT_LSTM әдісін пайдалану барысында басқа алгоритмдерге қарағанда жақсы нәтиже берді.

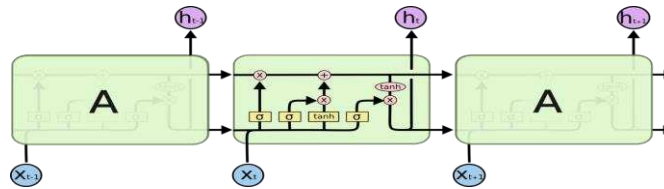


Сурет 2.11 – POLIT_LSTM әдісінің барлық метрикалар бойынша нәтижесі



Сурет 2.12 – POLIT_LSTM әдісі арқылы жіктеудің дәлсіздік матрицасы мен ROC қисық түріндегі нәтижесі

LSTM (Long short-term memory) жоғалып бара жатқан градиент мәселесін шешуге арналған және дәстүрлі RNN-мен салыстырғанда ақпаратты ұзақ уақыт сақтауға мүмкіндік береді. Сондықтан, біз дәстүрлі RNN нейрондық желіні емес, LSTM қолданамыз [31]. Төменде LSTM архитектурасы көрсетілген (сурет 2.13).



Сурет 2.13 – LSTM архитектурасы

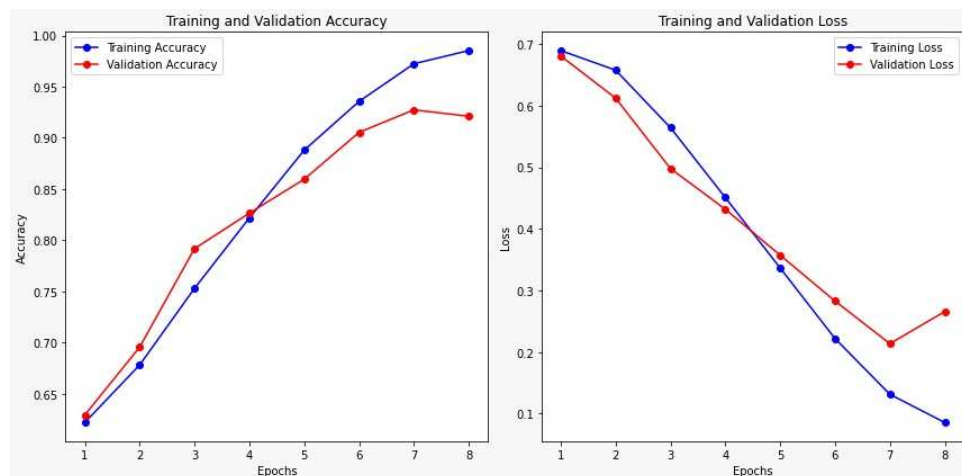
Ұзақ қысқа мерзімді жады (LSTM) бар терең оқыту желісінің көмегімен мәтіндік деректерді жіктейтін боламыз. Мәтіндік деректер табиғи түрде дәйекті. Мәтін бөлігі - бұл сөздер тізбегі, олардың арасында тәуелділіктер болуы мүмкін. Ұзақ мерзімді тәуелділікті үйрену және реттілік деректерін жіктеу үшін біз LSTM нейрондық желісін қолданамыз. LSTM желісі - жоғарыда көрсетілгендей реттілік деректерінің уақыт қадамдары арасындағы ұзақ мерзімді тәуелділікті үйрене алатын қайталанатын нейрондық желінің (RNN) түрі [32].

LSTM желісіне мәтін енгізу үшін алдымен мәтіндік деректерді сандық тізбектерге түрлендіру қажет. Нейрондық желі моделін құру кезінде біз мәтінді сандық мәндерге айналдырдық. Әрі қарай сол сандық мәндермен жұмыс істейміз.

Біз осы нейрондық желі үшін CNN нейрондық желі сияқты дәл сол модельді жасадық. Тек конволюциялық қабаттың орнына екі жақты LSTM қабаты қосылды.

Bidirectional LSTM дәстүрлі LSTM кеңейтімі болып табылады, ол реттілікті жіктеу тапсырмаларында модель өнімділігін жақсарта алады. Кіріс тізбегінің барлық уақыт аралықтары қол жетімді тапсырмаларда екі бағытты LSTM кіріс тізбегінде бір емес, екі LSTM жаттықтырады. Біріншісі кіріс тізбегін сол күйінде, ал екіншісі кіріс тізбегінің төңкерілген көшірмесін білдіреді. Бұл желіге қосымша контекст беріп, мәселені тезірек және одан да толық зерттеуге әкелуі мүмкін. Генеративті терең оқытудың осы түрімен шығыс деңгейі бір уақытта кері және тікелей күйлерден ақпарат ала алады.

LSTM қайталанатын желі моделін оқытудың 8 дәуірінде біз келесі нәтижеге қол жеткіздік (сурет 2.14):



Сурет 2.14 – Оқытудың 8 дәуіріндегі нәтиже

Алынған нәтижелер.

Осы тараудың нәтижесінде,

а) мәтіндік мазмұндағы экстремизмді анықтау тапсырмасына машиналық оқытудың әртүрлі үлгілері қолданылды;

б) берілген тапсырма үшін оңтайлы әдісті таңдау үшін машиналық оқыту әдістеріне салыстырмалы талдау жүргізілді;

в) деректердің теңгерімсіздігі мәселесін жою үшін артық іріктеу және жеткіліксіз таңдау әдістері жүргізілді;

г) қазақ мәтіндеріндегі экстремизмді анықтау үшін терең оқыту моделі әзірленді.

2.2 Әлеуметтік желілерінің графикалық ресурстарын өңдеу моделі

Көп жағдайда әлеуметтік желілердегі графикалық мазмұны монохромды немесе түрлі-түсті кескіндерден, сондай-ақ монохромды немесе түсті форматта ұсынылған моно-арналық бейнеден тұрады. Мысал ретінде сурет 2.15 – те саяси экстремизмге шақырудың иллюстрациясы болуы мүмкін сурет көрсетілген.



Сурет 2.15 – Көшедегі тәртіпсіздіктерге шақыру ретіндегі ұрыс көрінісі

Статикалық бейнелер мен бейне ақпараттарды нейрондық желіні талдау саласындағы практикалық тәжірибе мен зерттеу нәтижелері көрсеткендей [33, 34, 35], мұндай талдаудың тиімділігін арттырудың перспективалы жолдарының бірі алдын ала өңдеуді жүзеге асыру болып табылады. Ең алдымен, мұндай өңдеудің мақсаты кескіндер мен бейне ағындарының параметрлерін берілген типтегі нейрондық желі моделінің енгізу өрісінің параметрлеріне қойылатын талаптарға жеткізу. Осылайша, нейрондық желі моделінің кіріс өрісінің өлшемі мен талданатын кескіннің өлшемі арасындағы елеулі айырмашылық кескінді масштабтау үшін арнайы процедураны қолдануды талап етеді, өйткені тривиальды масштабтау процедурасы кескінді шамадан тыс бұрмалауы мүмкін.

Бұрмалау әсіресе кескіннің мүмкін болатын пропорционалды емес масштабтауы жағдайында байқалады, бұл қажеттілік нейрондық желі моделінің кіріс өрісінің арақатынасы мен талданатын кескіннің арақатынасы арасындағы сәйкессіздік жағдайында туындауы мүмкін.

Мысал ретінде сурет 2.16 – да сурет 2.15 – тің бикубтық интерполяция процедурасының көмегімен біркелкі емес масштабталған суреті кескенділген. Сурет 2.16-да мұндай масштабты кескінде адамдар тану қиын болатынын көрсетеді, сондықтан нейрондық желіні талдау да қиын болады.



Сурет 2.16 – Бикубтық интерполяция процедурасы арқылы кескінді масштабтау

Сонымен қатар, кейбір желідегі әлеуметтік желілерде кескіндер мен бейнелер сығылған түрде орналастырылғанын ескеру қажет, бұл оларды нейрондық желіні талдау құралдарының енгізуіне жіберу кезінде қиындықтар тудыруы мүмкін.

Сондай-ақ, көптеген жағдайларда кіріс сигналын алдын ала өңдеу жаттығулар деректерінде көрсету қиын шу мен бұрмалауды теңестіру арқылы нейрондық желі моделінің шығыс сигналының дәлдігін айтарлықтай арттыруы мүмкін. Мысал ретінде сурет 2.17-де тұманның әсерінен жарық аз жағдайда түсірілген адамдар тобының суреті көрсетілген.



Сурет 2.17 – Жарық аз жағдайда түсірілген адамдар тобының суреті

Сурет 2.18-де көрсетілгендей, бейне ағыны жеке кескін кадрларынан тұрады. Сондықтан бейне ағынын өңдеу бұл процесті нақты уақыт режимінде жүзеге асыру қажеттілігін ескере отырып, жеке суреттерді өңдеу ретінде қарастырылуы мүмкін.



Сурет 2.18. Бейне ағынын жеке кадрлар ретінде көрсету

Осылайша, бірінші жуықтау үшін желідегі әлеуметтік желілерде кескінді алдын ала өңдеудің негізгі міндеттері мыналарға қатысты:

1. Сығылған кескінді қалпына келтіру.
2. Кескіндерді олардың өлшемін нейрондық желі моделінің енгізу өрісінің өлшеміне келтіру үшін масштабтау.
3. Суреттерді берілген түсті пішімге келтіру.
4. Интернеттегі әлеуметтік желілердегі саяси экстремизм саласына тән типтік араласулар мен бұрмалауларды теңестіру.

Алғашқы үш тапсырма кескіндерді берілген типтегі нейрондық желі үлгісіне беру алдында алдын ала өңдеудің типтік тапсырмалары екенін ескеріңіз. Төртінші тапсырма қолданбалы зерттеу мәселесінің ерекшеліктерін ескереді, яғни мәтіндік және графикалық ақпаратты интегралды талдау арқылы онлайн әлеуметтік желілерде саяси экстремизмді анықтау міндеттері.

Алғашқы төрт мәселені шешудің тиімді жолдарын анықтау үшін кейбір кең таралған онлайн әлеуметтік желілерде суреттер мен бейне ағындарын орналастыру ерекшеліктеріне қатысты зерттеу жүргізілді. Қазіргі уақытта онлайн әлеуметтік желілердің саны өте көп болғандықтан, беделді Profit.kz сайтында 2023 жылдың 27 сәуірінде жарияланған «Қазақстандағы әлеуметтік желілердің рейтингі және олардан сатып алушылар не күтеді» атты мақаласы негізге алынды. Сауалнамаға қатысқандардың 56%-ы әлеуметтік желіде бейнелерді көріп, музыка тыңдайтыны, респонденттердің 44%-ы жаңалықтар оқитыны, 26%-ы бұрыннан танитын адамдармен араласатыны, 26%-ы блогерлерді бақылайтыны атап өтілген. Бұл ретте контенттің негізгі тұтынушылары 14 пен 18 жас аралығындағы жастар.

Қазақстан Республикасындағы онлайн әлеуметтік желілерге қатысуды сипаттайтын мақалада анықталған негізгі көрсеткіштер кесте 2.2 – де келтірілген.

Кесте 2.2 – Қазақстан Республикасындағы әлеуметтік желілерді қолдану көрсеткіші

| Әлеуметтік желі атауы | Жас көрсеткіші | Танымалдылығы, % |
|-----------------------|----------------|---------------------|
| Instagram | 14-35 жас | 71 |
| TikTok | | 59 |
| Telegram | | 57 |
| YouTube | | 57 |
| ВКонтакте | | 27 |
| Facebook | | 13 |
| Одноклассники | 25-35 жас | 8 |
| Twitter | | 3 |

Практикалық тәжірибені ескере отырып, кесте 2.2 – те көрсетілген онлайн әлеуметтік желілер тізіміне қосымша LinkedIn, Viber және WhatsApp платформалары қосылды. Көрсетілген тізімдегі әлеуметтік желілер суреттер мен бейне ағындарды алдын ала өңдеуге байланысты жоғарыда айтылған мәселелерді шешу жолдарын анықтау тұрғысынан зерттелді. Белгілі бір әлеуметтік желідегі ең көп таралған кескін және бейне параметрлері ғана ескерілді.

Instagram желісіндегі сурет: пост үшін квадрат сурет 1080 × 1080 px, пост үшін тігінен сурет 1080 × 1350 px, Stories үшін сурет 1080 × 1920 px, IGTV үшін мұқаба 1080 × 1920 px, Reel үшін мұқаба 1080 × 1920 px, профиль суреті 110 × 110 px кем емес. Файлдар форматтары: png, jpg, gif. Сурет жақтауларының қатынасы: 1:1; 1.91:1; 4:5.

Instagram желісіндегі бейнелер. Тік бейнелер үшін ажыратымдылығы 600 × 750 px – ден бастап 1080 × 1350 px дейін. Жақтаулар қатынасы: 4:5. Көлденең бейнелер үшін ажыратымдылық - 600 × 315 px басталып, 1080 × 566 px дейін, жақтаулар қатынасы 1,91:1 тең. Форматтар: MP4, MOV, FLV, WMV. Қолданылатын кодек H.264.

TikTok желісіндегі сурет: профиль фото 100 × 100 px, ұлғайту мүмкіндігімен 200 × 200 px, бейне иллюстрациялар үшін 1080 × 1920 px. Аватар кескіндерін пайдалану үшін 20 × 20 px. Файлдар форматтары: png, jpg.

TikTok желісіндегі бейнелер. TikTok желісінде ұсынылатын бейне ажыратымдылығы 1080 × 1920 px. TikTok бейне арақатынасы 9:16 немесе 1:1 бүйірлік панельдерімен болуы керек. Сонымен қатар, TikTok бейнелер өрісі оңынан және солынан 64 пиксель және жоғарыдан және төменнен 150 пиксель болуы қажет. TikTok көлденең бейнелерді қабылдайтынына қарамастан тік бейнелерді қолдану ұсынылады. Файлдар форматы: mov, mp4, avi, mpeg, 3pg. Қолданылатын кодек H.264.

Telegram желісіндегі сурет: профиль немесе канал суреті 640 × 640 px; пост

мұқабасы: 640 × 480 px, 800 × 400 px немесе 800 × 800 px. Суреттің максималды өлшемі: ені 5000 px – ге дейін, биіктігі 3000 px – ге дейін. Суреттер файлдарының форматтары: jpg, gif, png, tiff, webp, bmp.

Telegram желісіндегі бейнелер. Telegram арнасындағы пост үшін ұсынылатын бейне өлшемдері тік бейнелер үшін 3:2 немесе 2:3 арақатынасында болуы керек, яғни 1080 × 720 пиксель немесе 720 × 1080 px, 480 × 320 px немесе 320 × 480 px. H.264 және MPEG-4 кодектер мен контейнер ретінде пайдаланылады. Бейне файлының негізгі пішімдері: mp4, mov, wmv, avi, avchd, flv, f4v, swf, mkv, webm немесе html5.

Viber суреттері. Viber хабарламасында пайдалануға болатын ең үлкен кескін өлшемі 1600 × 1200 px, стандартты өлшемі - 600 × 600 px. Кескін файл пішімі: jpg, gif, png.

Viber бейне. Ұсынылатын ажыратымдылық 640×480 px, 1280×720 px немесе 1920×1080 px. Қолайлы бейне пішімдері - mp4, avi немесе mov. H.264 кодекі бар MP4 ұсынылады. Бейненің арақатынасы жоспарланған көру әдісін ескере отырып таңдалады. Viber екі негізгі арақатынасын қолдайды: 16:9 және 4:3. Жалпы бейне жазбалар үшін 16:9 арақатынасын пайдалануды ұсынамыз, себебі бұл көптеген заманауи құрылғылар үшін стандартты қатынас.

WhatsApp суреттері. WhatsApp jpg, jpeg және png кескін пішімдерін қолдайды. Оңтайлы көрсету үшін баннерлер өлшемі кемінде 600 × 600 px, ең үлкен өлшемі 1600 × 1200 px болуы керек. WhatsApp профиль суреті: экраны 4 дюймден аз смартфондар үшін 192 × 192 px немесе 140 × 140 px. Топтық диалог профилі үшін кескін өлшемі 192 × 192 px. WhatsApp Stories үшін ұсынылатын өлшем - 750 × 1334 px. Кескін пішімі jpg және png санаттарында болуы керек. Суреттер шаршы пішінді.

WhatsApp бейне. WhatsApp-та mp4, avi, flv, avi, wmv, mkv, 3gp, mov, vob кеңейтімі бар бейнелерді ойнатуға болады. Бейнелерді mp4 форматында жіберу ұсынылады. Қысқа бейнелер үшін ұсынылатын кадр биіктігі - 360 px немесе 480 px, ұзын бейнелер үшін - 240 px. Максималды ажыратымдылық 1280 × 720 px.

YouTube желісіндегі суреттер. Бейненің жоғарғы жағындағы сурет: 1280 × 720 px, арна мұқабасының минималды өлшемі 2048 × 1152 px, арна мұқабасының максималды өлшемі 2560 × 1440 px, профиль фотосы 800 × 800 px, Shorts мұқабасы 1920 × 1080 px. Пікірлер арақатынасы 16:9. Ұсынылатын файл пішімі - jpg және png.

YouTube желісіндегі бейне. Сатуға немесе жалға алуға арналған бейнелердің ажыратымдылығы кемінде 1920x1080 px, арақатынасы 16:9 болуы керек. Жарнамасы бар немесе жоқ мазмұн үшін YouTube ең төменгі ажыратымдылықты орнатпайды, бірақ 16:9 арақатынасы үшін кемінде 1280x720 px және 4:3 арақатынасы үшін кемінде 640x480 px ұсынады. YouTube 8 бейне форматтарын қолдайды: mp4, avi, wmv, mov, 3gp, flv, mpeg-1,2, webm. Стандартты 16:9 арақатынасы бар бейнелер үшін келесі ажыратымдылықтар пайдаланылады: 7680 × 4320 px, 3840 × 2160 px, 2560 × 1440 px, 1920 × 1080 px, 1280 × 720 px, 804 × 64 px, 854 × 60 px, 426 × 240 px.

ВКонтакте желісіндегі суреттер. Ұсынылатын өлшемдер. Сыртқы сілтемеге арналған сурет: 510×228 px; қауымдастық мұқабасы: 1590×530 px; жазбалар үшін сурет: 510×510 px (тікбұрышты кескінмен, арақатынасы 3:2); ВКонтакте тарихына арналған сурет: 1080×1920 px; клиптерге арналған мұқаба: 1080×1920 px; профиль фотосы: 200×500 px; айналмалы галерияға арналған суреттер (карусель): 400×400 px кем емес; әмбебап посттарға арналған сурет: 510×510 px (тікбұрышты кескінмен, арақатынасы 3:2); Сайттың сол жағындағы жарнамаға арналған сурет: мәтіні бар сурет 145×85 px, «үлкен сурет»: 145×165 px; қауымдастық немесе қолданба логотипі: 145×145 px; веб-сайтты жарнамалауға арналған сурет: логотиптің минималды өлшемі 256×256 px; үзінді үшін ең төменгі өлшем: 1080×607 px, арақатынасы 16:9); сюжеттерде жарнамаға арналған сурет: арақатынасы 9:16, өлшемі 720×1280 px кем емес. Кескін файл пішімі: jpg, png немесе gif (анимациясыз).

ВКонтакте желісіндегі бейне. Пост үшін ұсынылатын бейне ажыратымдылығы 1280×720 px немесе 1920×1080 px арақатынасы 16:9, ал бейнеклиптер үшін ұсынылатын ажыратымдылық - бірдей арақатынастағы 720×1280 px. 4К дейінгі бейне ажыратымдылығына қолдау көрсетіледі.

Жарнамаға арналған бейнежазбалардың параметрлері: арақатынасы - 1:1, 4:5, 16:9, 9:16; ең аз ені - 600 px; бейне форматы - mp4, mpeg, avi, mov; бейне кодек Н.264, ең төменгі ажыратымдылық 640×360 , ұсынылатын ажыратымдылық 1280×720 немесе 1920×1080 .

Қолдау көрсетілетін пішімдері: avi, mp4, 3gp, mpeg, mov, mp3, flv, wmv, mkv, ts, vob.

LinkedIn суреттері. Сыртқы сілтемелерге арналған сурет 1200×627 px, постқа арналған сурет 1080×1920 px, мұқаба 1584×396 px, профиль суреті: 400×400 px. 16:9 қатынасы.

LinkedIn бейне. LinkedIn Native бейнелері тік немесе көлденең болуы мүмкін. Тік бейнелер автоматты түрде жаңалықтар арнасындағы шаршыға қиылады. Бастапқы бейне үшін қолайлы арақатынасы 1:2,4 немесе 2,4:1. Ажыратымдылығы 256×154 px - ден 4096×2304 px дейін. Қолдау көрсетілетін бейне форматтары: avi, mp4, mkv, flv, mpeg-4, mpeg-1, asf, webm, quicktime, wmv2, wmv3, vp8, vp9. Ұсынылатын кодек – Н.264.

Одноклассниктегі суреттер. Жазбаның максималды кескін өлшемдері 1680×1680 px, мұқаба суреті 1944×600 px, профиль фотосы: 190×190 px. 900×600 px немесе 1200×800 px рұқсаты бар төртбұрышты пішімдегі жазбалар үшін кескіндерді пайдалану ұсынылады. Мақсатты жарнама: жарнамалық сілтеме өлшемдері - 640×320 px - ден (2:1); карусельдер - 600×600 px; көп форматта - 1080×607 px (1,78: 1); баннер - 240×400 px (3: 5); тизер - 90×75 px (6: 5). Қолдау көрсетілетін пішімдері: jpg, png.

Одноклассниктегі бейне. Рұқсат етілген бейне ажыратымдылығы - 640×360 px, 1280×720 px немесе 1920×1080 px. Әлеуметтік желі барлық танымал бейне файл пішімдерін қолдайды: mpeg, webm, mov, mp4, mxf, flv, svcd, vob, m2ts, dat, 3g2, m2v, mpe, avi, wm, rmvb, m4v, mpg, ts, 3gp, mkv, asf, vcd dv, wmv, m2p,

evo, divx, mcf, qt, f4v, ogg, rm, ogm.

Facebook суреттері. Ұсынылатын кескін өлшемдері: пост үшін 1200×630 px; сыртқы сілтеме суреті: 1080×1080 px; Facebook парақшасының мұқабасы: 820×312 px; Facebook Stories үшін: 1080×1920 px; профиль фотосы: 170×170 px; оң жақ бағандағы баннер және кіріс хабарламалар: 1200×1200 px; Facebook, Facebook Marketplace және жарнамалық хабарламалардағы жылдам мақалалар үшін: 1200×1200 px. Кескіннің арақатынасы: Facebook арнасының жарнамасы үшін: 1,91:1-ден 4:5-ке дейін; Сыртқы сілтеме суреті: 1,91:1 - 1:1; оң жақ бағандағы баннер және кіріс хабарламалар: 16:9-дан 1:1-ге дейін; Facebook Instant Articles, Facebook Marketplace және демеуші жазбалар үшін: 9:16-дан 16:9-ға дейін; сілтемемен жарияланған кезде: 1:1; Facebook Stories үшін: 1.91-ден 9:16-ға дейін. Facebook желісінде қолданылатын суреттер үшін кескіннің шамамен 14% бос қалдыру ұсынылады. Ол үшін суреттің жоғарғы және төменгі жағына мәтінді, логотипті және суреттің басқа негізгі элементтерін қоймау керек. Кескін файл пішімдері: jpg, png, gif.

Facebook бейне. Бейне параметрлері оның локализациясының орнына байланысты: Facebook арнасы, Facebook Marketplace, Facebook желісіндегі In-stream бейне жарнамасы, Facebook Stories.

Facebook арнасына арналған бейне параметрлері: ұсынылатын бейне өлшемдері - альбомдық және портреттік бағдар үшін 1280×720 px; ең төменгі ені - 600 px (ұзындығы арақатынасына байланысты) пейзаждық және портреттік бағдарлау үшін; ландшафт арақатынасы - 16:9; портрет арақатынасы 9:16 (егер бейнеде сілтеме болса, арақатынасы 16:9).

360 форматындағы бейне: максималды өлшемдері - 4096×2048 px; ең аз ені 600 px (ұзындық арақатынасына байланысты); арақатынасы 2:1.

Бейне параметрлері Жұмыс үстелі жаңалықтар арнасының сілтемесі Бейне (пейзаж, шаршы және оң жақ баған): ұсынылатын өлшемдер - 1280×720 px (пейзаж, шаршы); минималды өлшемдер 600×315 px (1,9:1 пейзаж) немесе 600×600 px (шаршы); ландшафт арақатынасы - 16:9.

Карусельдегі бейне параметрлері: ұсынылатын өлшемдер - пейзаж және шаршы үшін 1080×1080 px; ең аз өлшемдер 600×315 px (1,9:1 пейзаж) немесе 600×600 px (шаршы).

Бейне жарнамалар жинағы: ұсынылатын бейне өлшемдері - пейзаж және шаршы үшін 1200×628 px; минималды өлшемдер 600×315 px (1,9:1 пейзаж) немесе 600×600 px (шаршы); ландшафт арақатынасы - 16:9.

Facebook желісіндегі слайд-шоу: ұсынылатын өлшемдер – пейзаж және портреттік бағдарлау үшін 1200×720 px; ландшафт арақатынасы - 16:9; Портрет арақатынасы 9:16 (егер бейнеде сілтеме болса, арақатынасы 16:9).

Facebook Stories: ең төменгі өлшемдері - 500×500 px; арақатынастары - 1,9:1-ден 9:16-ға дейін. Ұсынылатын бейне пішімдері - mp4 және mov.

Twitter желісіндегі суреттер. Tweet суреті: 1024×512 px, мұқаба суреті: 1500×500 px, профиль суреті: 400×400 px.

Твиттердегі бейне. Twitter үшін көлденең бейнелерге арналған техникалық

сипаттамалар: mp4 пішімі, ұсынылатын өлшемі 1280 × 1024 px, ең аз өлшемі 32 × 32 px, максималды өлшемі 1920 × 1200 px, арақатынастары: 1:2,39 – 2,39:1. Ұсынылатын өлшем 1280 × 720 px. Ұсынылатын файл пішімдері mp4 немесе mov. Зерттеу нәтижелері көрсеткендей, ең танымал әлеуметтік желілер jpg, png, gif, bmp форматындағы суреттерді пайдаланады. Ең көп таралған бейне пішімдері mp4 және mov, ал пайдаланылатын пішімдердің тізіміне мыналар кіреді: mpeg, webm, mov, mp4, mxf, flv, svcd, vob, m2ts, dat, 3g2, m2v, mpe, avi, wm, rmvb, m4v, mpg, ts, 3gp, mkv, asf, vcd dv, wmv, m2p, evo, divx, mcf, qt, f4v, ogg, rm, ogm. Сондай-ақ кескіндер мен бейнелер үшін максималды және ең төменгі ажыратымдылық мәндерінің тізімі, кескіндер мен бейнелер үшін рұқсат етілген арақатынас диапазоны анықталды. Кесте 2.3 және 2.4 – те нақты деректер келтірілген.

Кесте 2.3 – Танымал әлеуметтік желілердегі суреттер мен бейнелердің максималды және минималды ажыратымдылығы

| Әлеуметтік желілер атауы | Максималды ажыратымдылық, px | Ұсынылатын минималды ажыратымдылық, px |
|--------------------------|------------------------------|--|
| Instagram | 1080 × 1920 | 110 × 110 |
| TikTok | 1080 × 1920 | 20 × 20 |
| Telegram | 720 × 1080 | 320 × 480 |
| Viber | 1600 × 1200 | 640 × 480 |
| WhatsApp | 1600 × 1200 | 192 × 192 |
| YouTube | 3840 × 2160 | 426 × 240 |
| ВКонтакте | 1920 × 1080 | 145 × 85 |
| LinkedIn | 4096 × 2304 | 256 × 154 |
| Одноклассники | 1920 × 1080 | 190 × 190 |
| Facebook | 4096 × 2048 | 170 × 170 |
| Twitter | 1920 × 1200 | 32 × 32 |

Кесте 2.4 – Танымал әлеуметтік желілердегі суреттер мен бейнелердің арақатынас диапазоны

| Әлеуметтік желілер атауы | Суреттер мен бейнелердің рұқсат етілген арақатынасы |
|--------------------------|---|
| Instagram | 1:1; 1,9:1; 4:5 |
| TikTok | 1:1; 9:16 |
| Telegram | 1:1; 2:3; |
| Viber | 1:1; 6:9; 4:3 |
| WhatsApp | 1:1; 4:3; 9:16 |
| YouTube | 4:3; 9:16 |
| ВКонтакте | 1:1; 2:3; 4:5; 9:16 |
| LinkedIn | 1:2,4; 9:16 |
| Одноклассники | 1:1; 1,78:1; 3:5; 6:5; 9:16 |
| Facebook | 1:1; 1,9:1; 2:1; 9:16 |
| Twitter | 1:1; 1:2,39; 9:16 |

Әдістеме негізінде [36], белгілі онлайн-әлеуметтік желілерді зерттеу нәтижелерін ескере отырып, сығылған кескіндерді және/немесе бейнелерді қалпына келтіруге байланысты жоғарыда аталған бірінші алдын ала өңдеу мәселесінің шешімін жалпыға ортақ пайдаланумен байланыстыруға болады. Бейнелерді олардың өлшемін нейрондық желі моделінің кіріс өрісінің өлшеміне келтіру үшін [37, 38] масштабтаумен байланысты екінші мәселенің шешімі қазіргі заманғы нейрондық желі модельдері бейнелерді адекватты түрде талдай алатындығы туралы дәлелдерге негізделген. пропорционалды түрде 2 еседен үлкейуі аспайды немесе пропорционалды түрде 5 еседен кішірейуі аспайды. Сондықтан, нейрондық желі моделіне бергенге дейін оларды алдын ала өңдеу кезінде кескіндер мен бейнелерді мақсатқа сай масштабтау шегі $k_{\max}=2$ және $k_{\min}=0,2$ коэффициенттерімен шектеледі, яғни пропорционалды масштабтаумен масштаб факторларының вариация диапазоны 0,2-ден 2-ге дейін. Пропорционалды емес масштабтау кезінде нейрондық желі модельдері 30%-дан [39, 40] аспайтын бұрмаланған кескіндерді талдауға қабілетті екенін ескеру қажет.

Сонымен қатар, кесте 2.5 – дегі деректер әлеуметтік желілердегі кескіндер мен бейнелердің өлшемдерінің өзгеру диапазоны көп жағдайда пропорционалды масштабтаудың белгіленген рұқсат етілген шектерінен айтарлықтай асып түсетінін көрсетеді. Кесте 2.5 – дегі деректер кесте 2.3 – тегі мәліметтерді тривиальды өңдеу нәтижесінде алынғанын ескерген жөн. Тек Telegram және Viber-тегі онлайн – әлеуметтік желілер үшін жалпы нейрондық желінің үлгісін қолдана отырып, нейрондық желіні талдауға кескіндерді дайындауға болады.

Кесте 2.5 – Әлеуметтік желілердегі суреттер мен бейнелердің өлшемін өзгерту

| Әлеуметтік желілер атауы | Максималды көлденең ажыратымдылықтың минимумға қатынасы | Максималды тік ажыратымдылықтың минимумға қатынасы |
|--------------------------|---|--|
| Instagram | 9,82 | 17,45 |
| TikTok | 54 | 96 |
| Telegram | 2,25 | 2,25 |
| Viber | 2,5 | 2,5 |
| WhatsApp | 8,33 | 6,25 |
| YouTube | 9,01 | 9 |
| ВКонтакте | 13,24 | 12,71 |
| LinkedIn | 16,00 | 14,96 |
| Одноклассники | 10,11 | 5,68 |
| Facebook | 24,09 | 12,05 |
| Twitter | 60 | 37,5 |

Сондай-ақ, кесте 2.4 – тегі деректерді талдау танымал әлеуметтік желілердегі суреттер мен бейнелердің арақатынасының айтарлықтай өзгермелілігін көрсетеді. Мысалы, Instagram 1:1 және 1,9:1 арақатынастары бар суреттерді орналастыра алады, бұл сондай-ақ осы кескіндерді нейрондық желіні талдау үшін жалпы нейрондық желі үлгісі пайдаланылса, кескіндерді масштабтау процедурасын айтарлықтай қиындатады.

Осылайша, зерттеулердің нәтижелері көрсеткендей, көп жағдайда, тіпті бір әлеуметтік желі ішінде, саяси экстремизмді тануға арналған жалпы нейрондық желі моделінің кіріс өрісіне бейімдеу үшін кескіндерді масштабтау өте қиын. Бір-бірінен ең алдымен енгізу өрісінің өлшемі бойынша ерекшеленетін бірнеше нейрондық желі модельдерін пайдалану техникалық күрделілігіне және бірнеше нейрондық желілерді оқыту қажеттілігіне байланысты тану жүйесінің тиімділігіне кері әсерін тигізетінін атап өткен жөн. Кескін өлшемдері 2,5 еседен аспайтын өзгертін жағдайларда (Telegram, Viber), тармағына сәйкес [41] масштабтау процедурасы бикубтық интерполяциялық аппаратқа негізделуі мүмкін.

Масштабтылықты тексерудің нақты процедурасын келесі өрнектер арқылы анықтауға болады:

$$k_x = \text{Round} \left(L_{NN} / L_{im} \right) \quad (2.1)$$

$$k_y = \text{Round} \left(H_{NN} / H_{im} \right) \quad (2.2)$$

$$\text{if } k_x \notin [k_{min}, k_{max}] \rightarrow \text{stop} \quad (2.3)$$

$$\text{if } k_y \notin [k_{min}, k_{max}] \rightarrow \text{stop} \quad (2.4)$$

$$\text{if } k_x / k_y > \partial \rightarrow \text{stop} \quad (2.5)$$

$$\text{if } k_y / k_x > \partial \rightarrow \text{stop} \quad (2.6)$$

мұндағы k_x, k_y – x және y осьтері бойынша масштабтық коэффициенттері; *Round* – ең кіші бүтінге дейінгі дөңгелектеу функциясы; L_{NN} – нейрондық желі моделінің енгізу өрісінің ені, H_{NN} – нейрондық желі моделінің кіріс өрісінің биіктігі; L_{im} – талданатын кескіннің ені; H_{im} – талданатын кескіннің биіктігі; k_{min}, k_{max} – ең төменгі және ең жоғары рұқсат етілген шкала коэффициентінің мәні; ∂ – осьтер бойынша масштабтаудың вариациясының максималды коэффициенті.

(2.3, 2.4) өрнектер пропорционалды масштабтау мүмкіндігінің шарттарын, ал (2.5, 2.6) өрнектер пропорционалды емес масштабтау мүмкіндігінің шарттарын анықтайтынын ескеріңіз.

Суреттерді берілген түсті пішімге келтіру мәселесін шешу талданатын кескіннің түс форматының қатынасына және нейрондық желі моделінің енгізу өрісінің түс форматына қойылатын талаптарға байланысты. Ықтимал опциялар:

1. RGB форматындағы түрлі-түсті кескінді RGBA форматына түрлендіру қажет;
2. RGBA форматындағы түрлі-түсті кескінді RGB форматына түрлендіру қажет;
3. Түсті кескінді жарты тонға түрлендіру қажет;

4. Түсті кескінді екілік жүйеге түрлендіру қажет.

Алғашқы екі нұсқаның шешімі кескін фонының мөлдірлігіне жауап беретін А-арнасын тривиальды түрде қосу/жою арқылы жүзеге асырылады.

Үшінші нұсқаның шешімі (2.7) өрнегінің көмегімен жүзеге асырылады.

$$C = 0,2125R + 0,7154G + 0,0721B \quad (2.7)$$

мұндағы С – жартылай реңк пішіміндегі пиксель түсі; R, G, B – әрбір RGB арнасындағы пикселдің түсін анықтайтын мәндер.

Төртінші нұсқаның шешімі (1.7-1.9) өрнектердің көмегімен жүзеге асырылады.

$$\begin{cases} \text{if } C \geq \alpha \rightarrow A = 1 \\ \text{if } C < \alpha \rightarrow A = 0 \end{cases} \quad (2.8)$$

$$\alpha = 0,5N \quad (2.9)$$

мұндағы α – шекті мән; N – жартылай тон пішіміндегі пиксель түсінің тереңдігі; A – екілік пішімдегі пиксель түсі.

Интернеттегі әлеуметтік желілердегі саяси экстремизм өрісіне тән типтік араласу мен бұрмалауды теңестіру мәселесін шешуді кескін сапасын түзету кезеңіне және кедергіден арылу кезеңіне бөлген жөн.

Ұқсастығы бойынша [42] кескін сапасын түзету сатысында түс арналарын қалыпқа келтіру, жарықтықты түзету және кескіннің контрастын түзету процедурасы жүзеге асырылады.

Кескіннің түс арналарын қалыпқа келтіру әрбір пикселдің түсінен осы арнаның орташа түс мәнін алып тастауды қамтитынын ескеріңіз:

$$\bar{C} = C - C_{cp} \quad (2.10)$$

мұндағы \bar{C} – нормаланған пиксель түсі, C – пикселдің бастапқы түсі; C_{cp} – берілген түс арнасындағы орташа түс мәні. Түс арналарының жарықтығын түзету процедурасы (2.11, 2.12) өрнектерге негізделген:

$$\Gamma(x, y) = \sum_{i=-a}^{0,5L} \sum_{j=-b}^{0,5H} (I(x+i, y+j) \times \Psi(x+i, y+j)), \quad (2.11)$$

$$\Psi = \begin{pmatrix} -2 & 0 & -2 \\ 0 & 9 & 0 \\ -2 & 0 & -2 \end{pmatrix} \quad (2.12)$$

мұндағы Γ – сүзгіленген сурет; I – бастапқы сурет; Ψ – сүзгі.

(2.11) өрнек мүмкін болатын сүзгі опцияларының біреуін ғана сипаттайтынын ескерген жөн. Контрастты түзету процедурасы (2.13-2.16) өрнектермен сипатталады.

$$\begin{cases} \text{if } g < r \rightarrow q = r \frac{1-f}{1+f} \\ \text{if } g = r \rightarrow q = g \\ \text{if } g > r \rightarrow q = r \frac{1+f}{1-f} \end{cases} \quad (2.13)$$

$$f = \left(\frac{|g - r|}{g + r} \right)^k \quad (2.14)$$

$$k = k_{min} + (k_{max} - k_{min})a \quad (2.15)$$

$$r = \frac{1}{d^2} \sum_{i=x-0,5d}^{x+0,5d} \sum_{j=y-0,5d}^{y+0,5d} c_{i,j} \quad (2.16)$$

мұндағы q – реттелген пиксель жарықтығының мәні; g – бастапқы пиксель жарықтығының мәні; r – пикселдің кейбір маңайының орташа жарықтығы; f – сызықты емес жергілікті контрастты күшейту функциясы; k – контрастты күшейту коэффициенті; k_{max}, k_{min} - максималды және минималды күшейту коэффициенті; a – пиксель маңайының сипаттамаларын ескере отырып бейімделу коэффициенті; d – пиксельдің көршілес диаметрі; x, y – контрастты реттеуді жүзеге асыратын пикселдің координаттары.

Ұсыныстарға сәйкес $k_{max} = 0,7 \dots 0,9$, $k_{min} = 0,1 \dots 0,3$, $d = 15 \dots 29$ пикселдер. Бірінші жуықтау ретінде қабылданған $k_{max} = 0,9$, $k_{min} = 0,2$, $a = 0,6$, $d = 20$ қабылданған. Болашақта бұл параметрлерді нақтылау үшін деректерді пайдалануға болады [43, 44].

(2.10-2.16) өрнектермен анықталған әзірленген процедураларды пайдалана отырып, сурет 2.17 – де көрсетілген аз жарық жағдайында жазылған адамдар тобының бейнесі өңделді. Өңдеу нәтижесі сурет 2.19 – да көрсетілгендей сурет 2.17 мен 2.19 – дегі сараптамалық салыстыру суретте көрсетілген жағдайды тану тұрғысынан әзірленген процедураларды орындау бастапқы кескіннің сапасын 5-10%-ға арттырғанын көрсетеді.



Сурет 2.19 – Жарық аз жағдайда түсірілген адамдар тобының өңделген суреті

Біркелкі емес жарықтандыру және/немесе бейнежазба қателеріне байланысты кескіннің айқын бұлыңғырлануы түрінде көрінетін бейне жазбаның әдеттегі кедергілерін теңестіру үшін [45] биометриялық параметрлерді сүзу үшін, қашықтықтан білім беру жүйелерінде қолдануға ұсынылатын тәсілге негізделген.

Әдістің мәні кейіннен үлкенірек вейвлет коэффициентін таңдай отырып, бейне кадрлардың толқындық коэффициенттерін жұптық салыстыру болып табылады. Тәсіл бейнежазбаның әртүрлі уақытында кескіннің әртүрлі бөліктерінде кедергі локализацияланғаны туралы практикалық мәлімдемеге негізделген. Мысал ретінде сурет 2.20 және 2.21 сәйкесінше кескіннің жоғарғы сол жақ және төменгі оң жақ бұрыштарында локализацияланған кедергі әсерінен көшедегі төбелестің көрінісі көрсетілген. Жекпе-жектің бастапқы бейнесі сурет 2.15 – те көрсетілгенін.



Сурет 2.20 – Бұлыңғырлық кескіннің жоғарғы сол жақ бұрышында локализацияланғаны



Сурет 2.21 – Бұлыңғырлық кескіннің төменгі оң жақ бұрышында локализацияланғандығы

$N \times N$ өлшемді квадрат кескіні жағдайында толқындық сүзгілеу моделін анықтайтын математикалық аппарат келесі өрнектермен анықталады:

$$\begin{cases} \mathbf{W}_{m,k} = \frac{1}{\sqrt{2^m}} \sum_{n=0}^{N-1} (c(x_n) \varphi^*(2^m x_n - k)), \\ 1 \leq m, k \leq N \end{cases} \quad (2.17)$$

$$\begin{cases} \mathbf{W}_{m,k}(i) = \frac{1}{\sqrt{2^m}} \sum_{n=0}^{N-1} (c(x_n, i) \varphi^*(2^m x_n - k)), \\ 1 \leq m, k \leq N \end{cases} \quad (2.18)$$

$$q(x_n) = \frac{\pi}{\ln(2)} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} (\varphi^*(x_n) \mathbf{W}_{m,k}), \quad (2.19)$$

$$q(x_n, i) = \frac{\pi}{\ln(2)} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} (\varphi^*(x_n) \mathbf{W}_{m,k}(i)). \quad (2.20)$$

$$\begin{aligned} \text{if } w(1)_{m,k} \geq w(2)_{m,k} &\rightarrow w(3)_{m,k} \\ &= w(1)_{m,k} \text{ else } w(3)_{m,k} = w(2)_{m,k} \end{aligned} \quad (2.21)$$

мұндағы \mathbf{W} – вейвлет-коэффициенттер матрицасы; $c(x_n)$ – жарты тонды кескін үшін x_n нүктесіндегі түс жарықтығы; $c(x_n, i)$ – түрлі түсті суреттер үшін i арналы түстің x_n нүктесіндегі жарығы, m, k - ауыстыру және масштабтау; x_n – кескінің n -ші нүктесінің координатасы; $*$ – кешенді жұптастыру операциясы; φ – базисты вейвлет; $w(1)_{m,k}$ – бірінші сурет үшін m, k -шы вейвлет коэффициенті; $w(2)_{m,k}$ – екінші бейне үшін m, k -ші вейвлет коэффициенті; $w(3)_{m,k}$ – үшінші сүзгіленген сурет үшін m, k -ші вейвлет коэффициенті;

(2.17) өрнек жарты тонды кескінің нүктелерінің бір қатарының толқындық коэффициенттерінің матрицасын анықтайтынын, ал (2.18) өрнек түсті кескінің i -ші түсті арнасы үшін бірдей матрицаны анықтайтынын ескеру қажет. Сүзу процесінің өзі (2.21) өрнегі арқылы жүзеге асырылады.

Сүзілген жартылай реңкті кескінді қалпына келтіру де (2.22) өрнек арқылы жүзеге асырылады. Түсті кескінді қалпына келтіру үшін (2.23) өрнек қолданылады.

$$q(x_n) = \frac{\pi}{\ln(a_0)} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} (\varphi^*(x_n) \mathbf{W}_{m,k}), \quad (2.22)$$

$$q(x_n, i) = \frac{\pi}{\ln(a_0)} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} (\varphi^*(x_n) \mathbf{W}_{m,k}(i)), \quad (2.23)$$

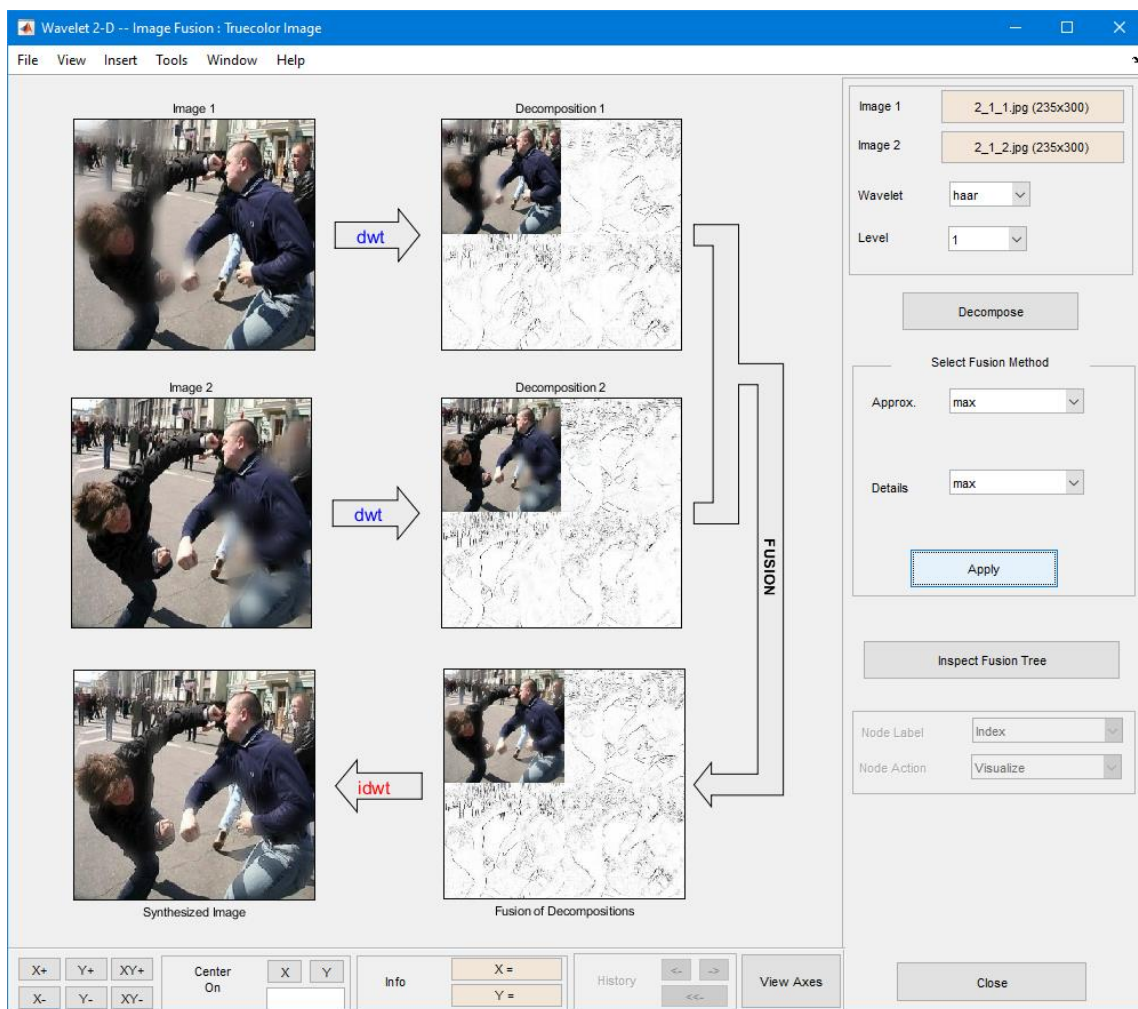
Шуды теңестіру үшін толқындық түрлендірулерді қолданудың белгілі

негізгі шешімінен айырмашылығы, бұл диссертациялық жұмыс (2.21) өрнекке негізделген сүзу процедурасын пайдалануды ұсынады, Хаар толқындарын базалық толқын ретінде пайдалану (2.24) өрнегімен, сондай-ақ толқындық түрлендірулердің егжей-тегжейлерінің бір деңгейімен анықталады.

$$\varphi = \begin{cases} 1, 0 \leq x < 0,5 \\ -1, 0,5 \leq x < 1 \\ 0, x \notin [0,1[\end{cases} \quad (2.24)$$

Фильтрлеу түрі (2.21) және вейвлет-Хаар үшін өрнекті пайдаланудың орындылығының негіздемесі сүзгілеу сапасының қолайлы деңгейінде есептеу ресурстарын азайту тұрғысынан жүзеге асырылатынын ескеріңіз.

Сурет 2.20 және 2.21 – де көрсетілген кескіндердің әртүрлі бөліктерінде локализацияланған бұлыңғырлықтарды жою үшін (2.17-2.24) өрнектермен көрсетілген сүзгілеу моделін пайдалану мысалы сурет 2.22 – де көрсетілген. Бұл жағдайда модель MatLab құралдарының көмегімен жүзеге асырылды.



Сурет 2.22 – Кескіннің әртүрлі бөліктерінде локализацияланған бұлыңғырлықты жою үшін сүзу үлгісін пайдалану иллюстрациясы

Осылайша, зерттеу нәтижесінде:

- Интернеттегі ең танымал әлеуметтік желілерде орналастырылған графикалық контенттің параметрлері анықталды: сурет сақталатын файл түрі, форматы, ажыратымдылығы және кескіннің арақатынасы;
- Саяси экстремизмді анықтау үшін онлайн-әлеуметтік желілерде суреттерді алдын ала өңдеудің негізгі міндеттерінің тізімі негізделген:
 1. Қысылған кескінді қалпына келтіру.
 2. Кескіндерді олардың өлшемін нейрондық желі моделінің енгізу өрісінің өлшеміне келтіру үшін масштабтау.
 3. Суреттерді берілген түс пішіміне келтіру.
 4. Интернеттегі әлеуметтік желілердегі саяси экстремизм саласына тән типтік араласулар мен бұрмалауларды теңестіру.
- Жалпыға қолжетімді бейне кодектерді қолдану арқылы бірінші алдын ала өңдеу мәселесін шешу мүмкіндігі көрсетілген.
- Екінші, үшінші және төртінші есептерді шешуге арналған (2.1-2.24) өрнектермен нақтыланған математикалық модель әзірленді. Ұсынылып отырған модельдің негізгі ғылыми жаңалығы желідегі әлеуметтік желілердегі кескіндердегі әдеттегі шуды сүзгілеуге арналған түпнұсқа толқындық түрлендіру аппаратын пайдалануында. Кескіндерді кейінгі талдау үшін нейрондық желі үлгісіне жібермес бұрын олардың жарықтығы мен контрастын түзетуге арналған математикалық аппаратты әзірлеу де қызығушылық тудырады.
- Танымал онлайн әлеуметтік желілердегі кескін өлшемдерінің үлкен өзгермелілігі бұл өлшемдерді шектеулі стандартты жиынтыққа дейін азайтуға мүмкіндік бермейтіні дәлелденді, саяси экстремизмді анықтауға арналған нейрондық желі моделінің архитектурасында осы мүмкіндікті ескеру қажеттілігін алдын ала анықтайды.

2.3 Онлайн әлеуметтік желілеріндегі графикалық ресурстарды талдаудың нейрожелілік моделі

Жалпы алғанда, желілік әлеуметтік желілердің графикалық ресурстарын талдау үшін нейрондық желі моделі арқылы жүзеге асырылатын ақпаратты түрлендіруді келесі өрнектер арқылы сипаттауға болады:

$$F_{NN}(GM) \rightarrow Y, \quad (3.1)$$

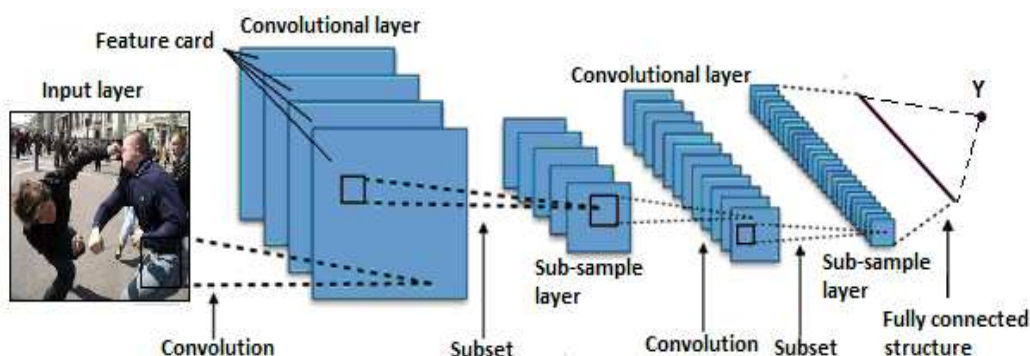
$$GM = \langle \{Im\}, \{Vd\} \rangle, \quad (3.2)$$

$$Y = \langle \{Y_{Im}\}, \{Y_{Vd}\} \rangle, \quad (3.3)$$

мұндағы F_{NN} – нейрондық желіні тану функциясы; GM – графикалық материалдар; Y – интернеттегі әлеуметтік желілердің графикалық материалында саяси экстремизмнің болуын көрсететін нейрондық желі моделінің шығуы; $\{Im\}, \{Vd\}$ – әлеуметтік желілердегі суреттер жиыны мен бейнелер жиыны; $\{Y_{Im}\}, \{Y_{Vd}\}$ – интернеттегі әлеуметтік желілердің суреттері мен бейнематериалдарында саяси экстремизмнің болуын көрсететін нейрондық желі

моделінің шығыс сигналдарын қамтитын жиындар.

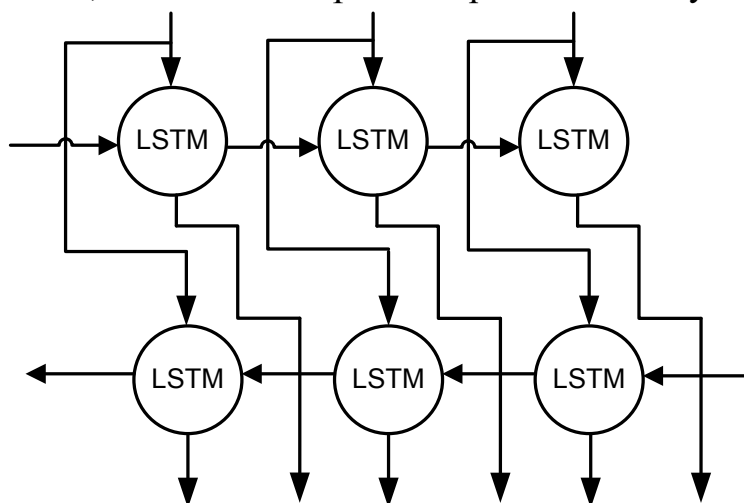
Графикалық ресурстарды нейрондық желіні талдау саласындағы заманауи жетістіктерге сүйене отырып [46] нейрондық желі моделінің негізгі түрі, растрлық кескінді талдау үшін кеңінен қолданылатын CNN нейрондық желі, оның классикалық құрылымы 2.23-суретте көрсетілген.



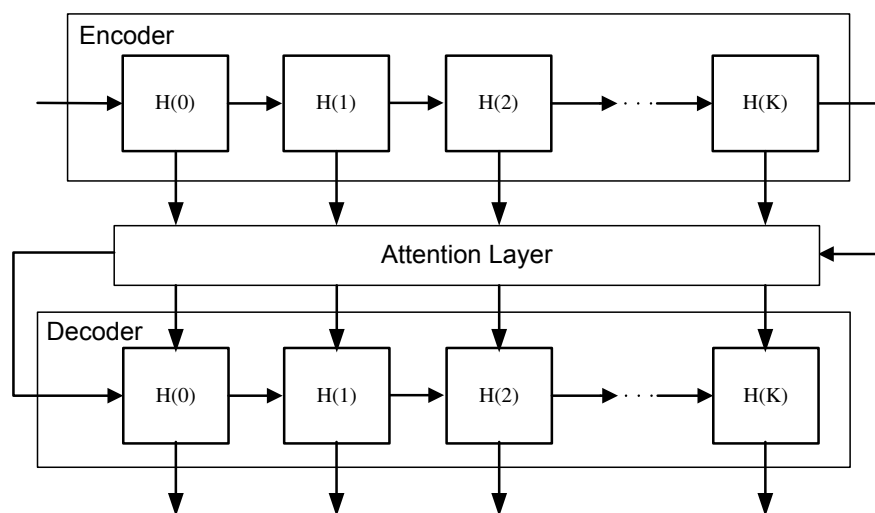
Сурет 2.23 – Интернеттегі әлеуметтік желілерде саяси экстремизмді тануға арналған классикалық CNN нейрондық желінің құрылымы

Сонымен қатар, бейнематериалдардың ерекшеліктерін есепке алу RNN нейрондық желілерді пайдалануды немесе attention механизмін сигналдың тікелей таралуымен нейрондық желіге немесе RNN нейрондық желіге біріктіруді қамтиды.

LSTM ұяшықтарына негізделген заманауи қайталанатын нейрондық желінің жалпыланған құрылымы сурет 2.24 – те, ал Attention механизмін іске асырудың құрылымдық схемасы сурет 2.25 – те көрсетілген. GPU ұяшықтарына негізделген нейрондық желінің құрылымы LSTM ұяшықтарына негізделген құрылымға ұқсас болады, басқа типтегі ұяшықтарды пайдалануды қоспағанда.



Сурет 2.24 – LSTM ұяшықтарына негізделген RNN нейрондық желінің құрылымы



Сурет 2.25 – RNN нейрондық желі үшін Attention механизмін енгізу

Айта кету керек, қазіргі уақытта CNN нейрондық желілердің әртүрлі модификациялары қолданылады, олардың сипаттамалары мен мүмкіндіктері бір-бірінен айтарлықтай ерекшеленеді. Сонымен қатар, нейрондық желі моделінің архитектурасын әзірлеу әдістемесі кеңінен танымал және жеткілікті түрде сыналған, оның параметрлері тапсырманы тиімді шешуге мүмкіндік береді [47, 48]. Осы әдіснаманы қолдана отырып, саяси экстремизмге шақыруларды анықтау тұрғысынан онлайн әлеуметтік желілердің суреттерінде CNN нейрондық желінің түрін таңдауға мүмкіндік беретін математикалық аппарат жасалды. Бұл математикалық аппараттың негізі өрнектері:

$$T_{CNN} = \max(\mathbf{E}), \quad (3.4)$$

$$\mathbf{E} = \{E_1, E_2, \dots, E_N\}, \quad (3.5)$$

$$E_i = \alpha_1 A_1(i) + \alpha_2 A_2(i) + \alpha_3 A_3(i), \quad (3.6)$$

мұндағы T_{CNN} – CNN нейрондық желінің ең тиімді түрі; \mathbf{E} – CNN нейрондық желілердің қол жетімді түрлеріне арналған интегралды тиімділік көрсеткіштері бар жиым; E_i – CNN нейрондық желінің i – типті интегралды тиімділік көрсеткіштері; N – CNN нейрондық желілердің қарастырылатын түрлерінің саны; $A_1(i), A_2(i), A_3(i)$ – CNN нейрондық желінің i типі үшін бірінші, екінші және үшінші тиімділік критерийлерінің мәндері; $\alpha_1, \alpha_2, \alpha_3$ – тиісінше бірінші, екінші және үшінші тиімділік критерийлерінің салмақ коэффициенті.

$A_1(i)$ критерийі тану дәлдігімен, $A_2(i)$ – критерийі танудың ресурс сыйымдылығымен, ал $A_3(i)$ – критерийі CNN нейрондық желінің i – типті оқу уақытымен байланысты екенін ескереміз.

Нәтижелеріне сүйене отырып [49], саяси экстремизмді тану міндетін графикалық материалды жіктеу міндеті ретінде ұсынуға болатындығын ескере отырып, дәлдік критерийін бағалау үшін Assurance көрсеткіші қолданылады, ол келесі өрнек арқылы есептеледі:

$$Ac = \frac{Nr}{N}, \quad (3.7)$$

мұндағы Nr – дұрыс танылған мысалдар саны; N – мысалдардың жалпы саны. Нейрондық желі моделінің дәлдігі әдетте жаттығу, сынақ және валидация үлгілерінде бағаланатындықтан, дәлдікті бағалау үшін өрнектің біршама өзгертілген түрі (3.7) қолданылады:

$$Ac_k = \frac{Nr_k}{N_k}, \quad k = 1, 2, 3. \quad (3.8)$$

(3.7) өрнегіндегі k мәні үлгі нөміріне сәйкес келеді:

$k = 1$ – жаттығу жиынтығы;

$k = 2$ – сынақ үлгісі;

$k = 3$ – валидация жинағы.

Нұсқауларға сәйкес [50], CNN нейрондық желіні тану дәлдігіне қатысты A_1 тиімділік критерийін бағалаудың қосымша параметрі ретінде өрнекпен анықталған Loss көрсеткіші пайдаланылды:

$$L = \frac{1}{N} \sum_{n=1}^N \sum_{q=1}^Q a_{n,q} \ln(y_{n,q}), \quad (3.9)$$

мұндағы N – мысалдардың жалпы саны; Q – танылуы керек класстар саны; $y_{n,q}$ – n -ші мысалды q -классқа жатқызуды көрсететін нейрондық желі моделінің шығыс сигналдарының мәндері.

Loss көрсеткішін қолданылатын мысалдар түріне бейімдеу қажеттілігін ескере отырып, (3.9) өрнек келесідей өзгертілген:

$$L_k = \frac{1}{N_k} \sum_{n=1}^{N_k} \sum_{q=1}^Q a_{n,q} \ln(y_{n,q}). \quad (3.10)$$

Теориялық нәтижелерге негізделі отырып, A_2 тиімділік критерийін бағалау үшін, танудың ресурс сыйымдылығымен байланысты өрнектер түрлері қолданылады:

$$A_2 = \rho \bar{N}_W, \quad (3.11)$$

$$\bar{N}_W = \frac{N_W}{N_W^{max}} \quad (3.12)$$

мұндағы ρ – берілген коэффициент; N_W – бағаланатын типтегі CNN нейрондық желідегі салмақ коэффициенттерінің саны; \bar{N}_W – бағаланатын типтегі CNN нейрондық желідегі салмақ коэффициенттерінің келтірілген саны; N_W^{max} – CNN нейрондық желілердің бағаланатын түрлері арасындағы салмақ коэффициенттерінің максималды саны.

CNN нейрондық желілердің ресурс сыйымдылығын салыстыруға байланысты бағалау есептеулерін жүргізген кезде, базалық нұсқада $\rho = const$ бағаланатын желілердің барлық түрлері үшін бірдей деп есептеледі. Осылайша, CNN нейрондық желінің белгілі бір түрінің ресурс сыйымдылығын бағалау

нейрондық желі моделінің осы түрінің салмақ коэффициенттерінің санын анықтаумен байланысты.

Нейрондық желі моделінің тиімділігін арттыру ресурс сыйымдылығының төмендеуімен байланысты болғандықтан, (3.11) өрнегінде ρ теріс мағына қолданылады.

CNN нейрондық желінің оқу уақытына қатысты A_3 тиімділік критерийі нейрондық желі моделінің салмақ коэффициенттерінің санына және нейрондық желі моделінің осы түріне тән оқыту механизмінің ерекшеліктеріне тікелей байланысты. Желіні оқытудың бір типті тетіктерін пайдаланған жағдайда, A_3 тиімділік критерийін бағалау үшін нейрондық желі моделі түрлерінің тиімділігін салыстыру мәселесінде (3.11) қолдануға болады.

CNN нейрондық желілердің көптеген рұқсат етілген түрлерін қалыптастыру оларды нейрондық желіні талдау тапсырмаларында сынақтан өткізу және ашық бағдарламалық коды бар қол жетімді аспаптық қамтамасыз етудің болуы тұрғысынан жүзеге асырылады, бұл мемлекеттің ақпараттық қауіпсіздігін қамтамасыз ететін жоғары жауапты жүйелерде пайдалану қажеттілігімен түсіндіріледі. Сайып келгенде CNN нейрондық желілердің көптеген қолайлы түрлеріне мыналар кірді: VGG-16, VGG-19, Inception, GoogleNet, MobileNetV2, SqueezeNet, ResNet:

$$T \quad (3.13)$$

$$= \{T_{VGG-16}, T_{VGG-19}, T_{Inception}, T_{GoogleNet}, T_{MobileNetV2}, T_{SqueezeNet}, T_{ResNet}\} \quad (3.4)$$

(3.4) - (3.13) өрнектерін пайдалана отырып жүргізілген есептеулер онлайн әлеуметтік желілердің кескіндеріндегі саяси экстремизмді анықтау міндетінде CNN нейрондық желілердің рұқсат етілген түрлерінің ішінде MobileNetV2 типті CNN нейрондық желілер ең үлкен тиімділікке ие екенін көрсетеді, олар үшін есептелген интегралды тиімділік көрсеткіші максималды мәнге ие. Есептеулерді жүргізу кезінде $\alpha_1 = 0,5$, $\alpha_2 = 0,25$, $\alpha_3 = 0,25$ екенін ескереміз.

MobileNetV2 негізінде "depthwise separable convolution" механизмі жатыр, ол 1x1 ядросы бар арналы конволюция болып табылатын depthwise-конволюция операциясын орындау үшін пайдаланылады [51, 52].

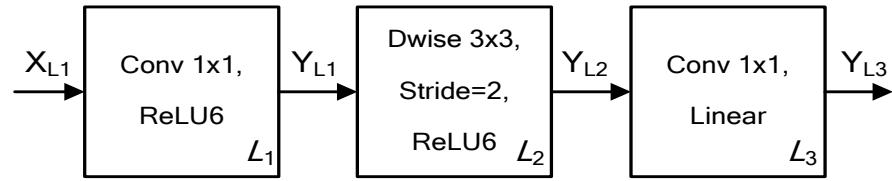
Мұндай конволюция "pointwise convolution" деп аталды. Көрсетілген механизмді қолдану арқылы CNN нейрондық желінің шығыс сигналын есептеу үшін қажетті есептеу операцияларының санын азайту әсеріне қол жеткізіледі. «depthwise separable convolution» механизмін пайдаланатын бір CNN қабатты пайдаланған жағдайда, классикалық CNN қабатқа қатысты есептеу операцияларының санының өзгеру коэффициентін келесідей есептеуге болады:

$$\delta = \frac{d^2 \times k_{out}}{d^2 + k_{out}} \quad (3.14)$$

мұндағы δ – өзгеріс коэффициенті; d – конволюция ядросының мөлшері; k_{out} – қабаттан шығатын арналар саны.

MobileNetV2 құрылымының айрықша ерекшелігі – кеңейту CNN блоктары деп аталатын модульдердің болуы. Мұндай блоктың құрылымы сурет 2.26 – да

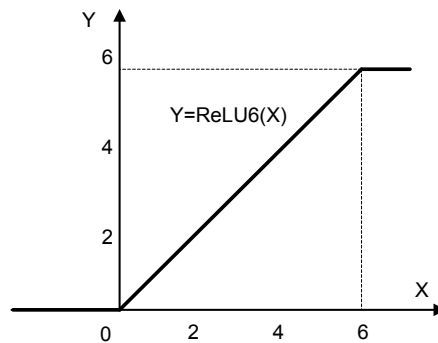
көрсетілген.



Сурет 2.26 – Кеңейту CNN блогының құрылымы

2.25-суретте келесі белгілер қабылданғанын ескерсек:

- L_1, L_2, L_3 – сәйкесінше 1, 2, 3 қабат.
- X_{L1} – L_1 үшін кіріс тензоры;
- Y_{L1}, Y_{L2}, Y_{L3} – L_1, L_2, L_3 қабаттарына арналған сәйкесінше шығыс тензорлары;
- Conv 1x1 – 1x1 конволюция ядросы бар конволюция;
- ReLU6 – (3.15) өрнегімен берілген белсендіру функциясы, оның графигі 2.27-суретте көрсетілген;
- Stride=2 – Конволюция ядросының 2 қадамымен ығысуы;
- Dwise 3x3 – 3x3 CNN ядросы бар терең (көп арналы) конволюция.



Сурет 2.27 – ReLU6 белсендіру функциясының графигі

Кеңейтетін CNN блоктағы ақпаратты өңдеу механизмі келесі өрнектермен сипатталады:

$$y = \begin{cases} 0, & \text{if } x \leq 0 \\ x, & \text{if } 0 < x < 6 \\ 6, & \text{if } x \geq 6 \end{cases} \quad (3.15)$$

$$K_{X_{L1}} = H^2 \times k_{L1} \quad (3.16)$$

$$K_{Y_{L1}} = H_{L1}^2 \times k_{L1} \times t \quad (3.17)$$

$$K_{Y_{L2}} = \frac{H_{L2}^2}{S^2} \times t \times k_{L2} \quad (3.18)$$

$$K_{Y_{L3}} = \frac{H_{L3}^2}{S^2} \times t \times k_{L3} \quad (3.19)$$

мұндағы x – белсендіру функциясының жалпы кіріс сигналы; y – белсендіру функциясының шығыс сигналы; $K_{X_{L1}}$ – L_1 қабаты үшін кіріс тензорының өлшемі; H – L_1 қабаты үшін шығыс тензорының өлшемі; k_{L1} – L_1

кабаты үшін кіріс тензоры арналарының саны; $K_{Y_{L_1}}, K_{Y_{L_2}}, K_{Y_{L_3}}$ - L_1, L_2, L_3 , үшін сәйкесінші шығыс тензорларының өлшемі; t – кеңейтілу деңгейі; $H_{L_1}, H_{L_2}, H_{L_3}$ – L_1, L_2, L_3 , үшін сәйкесінше шығыс тензорларының мөлшері; s - конволюция ядросының ығысуы.

Ұсынылған t мәндерінің диапазоны 5-тен 10-ға дейін. Бірінші жуықтау ретінде әдеттегідей $t=6$ қолданылады. Бұл жағдайда алдыңғы қабаттың шығыс тензоры келесі қабаттың кіріс тензоры болып табылады. Мәселен, $K_{Y_{L_1}}$ L_2 қабатының кіріс тензоры болып табылады. L_3 қабатының шығыс тензоры жеке модульдің шығыс тензоры болып табылады (кеңейту CNN блогы).

Сондай – ақ, классикалық нейрондық желілердің терминологиясында кіріс тензоры желінің және жеке қабаттың кіріс ақпаратымен, ал шығыс тензоры шығыс ақпаратымен байланысты екенін атап өткен жөн. CNN нейрондық желі терминологиясында кіріс тензоры желінің кірісіне, CNN қабатқа немесе масштабтау қабатына берілетін кескінмен байланысты. Шығыс тензоры CNN қабаттың, масштабтау қабатының немесе бүкіл желінің шығыс ақпаратымен байланысты.

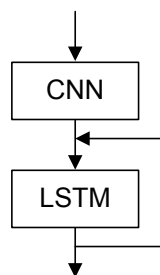
Зерттеудің келесі кезеңі интернеттегі әлеуметтік желілердегі бейнематериалдардағы саяси экстремизмге шақыруларды тануға арналған қайталанатын нейрондық желі моделінің ең тиімді түрін анықтауға арналды. Нәтижелерге негізделіп отырып [53, 54, 55], практикалық тәжірибеге сәйкес, қазіргі уақытта құрылымы 2.22-суретте көрсетілгендей LSTM-ұяшықтары мен GRU-ұяшықтарға негізделген қайталанатын нейрондық желілер ең тиімді болып саналады. Сонымен қатар, екі бағытты ассоциативті жад, Хопфилд, Хемминг, Джордан, Элман қайталанатын нейрондық желілері нейрондық желіні талдауға тән бейнематериалдардың ұзақ мерзімді тәуелділіктерін толық есепке алмау себебінен ескірген болып саналады.

Сонымен қатар, LSTM және GRU типті қайталанатын нейрондық желілерді теориялық зерттеу олардың салыстырмалы тиімділігін бағалаудың аналитикалық аппаратының жоқтығын көрсетеді. Тек GRU, LSTM желіге қатысты деректердің ұзақ тізбегін есте сақтай алатындығы көрсетілген. Сонымен бірге, LSTM – желісі GRU – ға қарағанда ресурстарды көп қажет етеді. Сондай-ақ, қол жетімді ғылыми-практикалық әдебиеттерде желідегі LSTM/GRU-ұяшықтары мен LSTM/GRU- қабаттарының оңтайлы санын анықтауға арналған аналитикалық аппарат жоқ.

Сондықтан желінің түрін, сондай-ақ LSTM/GRU – қабаттарының санын және әр қабаттағы LSTM/GRU – ұяшықтарының санын анықтау үшін эксперименттік зерттеулер жүргізу қажет [56, 57]. Мұндай зерттеулер барысында қайталанатын нейрондық желінің түрі мен параметрлерін анықтаған жөн, ол кең таралған онлайн әлеуметтік желілердің бейнематериалдарындағы саяси экстремизмді тиімді таниды. Сондай-ақ, нәтижелерді [58] пайдалана отырып, статикалық кескіндерді де, бейнематериалдарды да талдауға мүмкіндік беретін интегралды нейрондық желі моделін қолданудың орындылығы туралы алғышарт қабылданды.

Саяси экстремизмді танудың әмбебап құралдарын әзірлеу тұрғысынан мұндай нейрондық желі кем дегенде бір онлайн әлеуметтік желінің бейнелері мен бейнематериалдарын ұсыну ерекшеліктеріне бейімделуі керек.

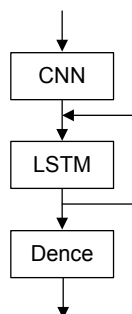
Ең алдымен, нейрондық желі моделі кескіндер мен бейне материалдардың өлшемдерінің өзгергіштігіне бейімделуі керек. Есептеу ресурстарына ықтимал шектеулерді, сондай-ақ кіріс кескінін немесе бейнені тиімді масштабтау мүмкіндігін ескере отырып, негізгі нұсқада 64x64 өлшемді нейрондық желі моделінің кіріс өрісін пайдалану ұсынылады. Негізгі нұсқада интегралды нейрондық желінің негізгі нұсқасының құрылымы сурет 2.28 – де көрсетілген. Пайдаланылған CNN нейрондық желінің ерекшелігі – шығыс қабатының болмауы, бұл қайталанатын нейрондық желінің кірісіне конволюцияның соңғы қабатына сәйкес келетін сигналдардың берілуіне әкеледі.



Сурет 2.28 – Кескін мен бейнені танудың негізгі интегралды нейрондық желілік моделінің құрылымы

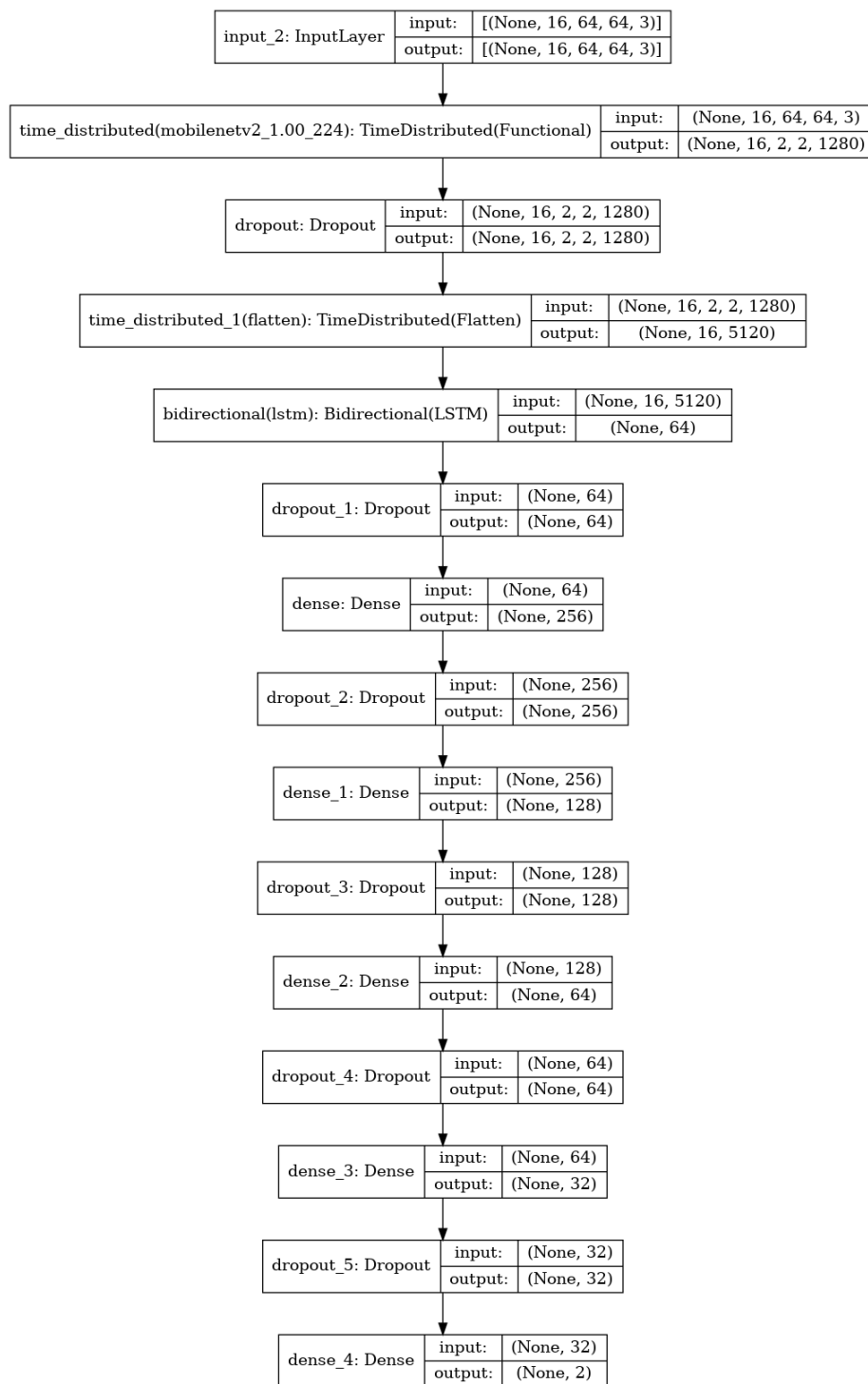
Сурет 2.28 – дегі белгілер: CNN – CNN нейрондық желі; LSTM – LSTM-ұяшықтарына негізделген екі бағытты RNN нейрондық желі.

Ұсыныстарға сәйкес [59], нейрондық желі моделі нейрондардың толық байланысқан қабаттарын қосу арқылы өзгертіледі, олардың қолданылуы тану дәлдігін арттырады. Нейрондардың бір немесе бірнеше толық байланысқан қабаттарына сәйкес келетін блок қосылған интегралды нейрондық желіні тану моделінің құрылымы сурет 2.29 – те көрсетілген, бұл блок Dense деп белгіленген.



Сурет 2.29 – Негізгі интегралдың құрылымы кескін мен бейнені танудың нейрондық желілік моделі толық байланысқан қабаттар блогымен толықтырылған.

Толық байланысқан қабаттардың санын, сондай-ақ толық байланысқан қабаттардың әрқайсысындағы нейрондардың санын эксперименттік зерттеулер арқылы анықтау керек екенін ескереміз, өйткені бүгінгі күні бұл шамаларды анықтайтын сенімді аналитикалық аппарат ашық қол жетімді емес. Сурет 2.29 – дағы жиынтық желіні MobileNetV2 типті бейімделген нейрондық желіге ауыстыру онлайн әлеуметтік желілердің графикалық нысандарындағы саяси экстремизмді тануда нейрондық желі моделінің жалпы құрылымын ұсынуға мүмкіндік берді. Мұндай желінің құрылымы сурет 2.30 – да көрсетілген.



Сурет 2.30 – MobileNetV2 негізіндегі интегралды нейрондық тану моделі

Сурет 2.30– да көрсетілген MobileNetV2 негізіндегі интегралды нейрондық тану моделінің құрылымы TensorFlow кітапханасының кіріктірілген құралдары арқылы көрсетілгенін ескереміз. Сондықтан сурет 2.30– да нейрондық желі модельдерінің құрылымын дәстүрлі түрде көрсету кезінде әдетте көрсетілмейтін элементтер көрсетілген. Мысалы, сурет 2.30– да dropout_5 модулі кірістірілген, ол нейрондық желі моделін оқыту процесінде үшінші толық байланысқан қабаттың салмақ коэффициенттерін есептеу кезінде dropout механизмі қолданылатынын көрсетеді. Сондай-ақ, классикалық CNN нейрондық желіден айырмашылығы, әзірленген модельдің кірісіне бейне ағынының 16 кадрын беру қарастырылғанын атап өткен жөн.

Әзірленген нейрондық желі моделінің негізгі параметрлері кесте 2.6-да келтірілген.

Кесте 2.6 – Интернеттегі әлеуметтік желілердің графикалық материалдарындағы саяси экстремизмді тану үшін қайталанатын және толық байланысқан нейрондық желі модульдерінің негізгі құрылымдық параметрлері

| Layer (type) | Output Shape | Param # |
|---------------------|-----------------------------------|---------|
| time_distributed | TimeDistri (None, 16, 2, 2, 1280) | 2257984 |
| dropout (Dropout) | None, 16, 2, 2, 1280 | 0 |
| time_distributed_1 | TimeDist (None, 16, 5120) | 0 |
| bidirectional | Bidirectional (None, 64) | 1319168 |
| dropout_1 (Dropout) | None, 64 | 0 |
| dense (Dense) | None, 256 | 16640 |
| dropout_2 (Dropout) | None, 256 | 0 |
| dense_1 (Dense) | None, 128 | 32896 |
| dropout_3 (Dropout) | None, 128 | 0 |
| dense_2 (Dense) | None, 64 | 8256 |
| dropout_4 (Dropout) | None, 64 | 0 |
| dense_3 (Dense) | None, 32 | 2080 |
| dropout_5 (Dropout) | None, 32 | 0 |
| dense_4 (Dense) | None, 2 | 66 |

Құрылған нейрондық желі моделінің қайталанатын және толық қосылған модульдеріндегі жобалық параметрлердің жалпы саны 3637090, оның ішінде модель архитектурасын құрастыру кезінде анықталған 576448 параметр және желілік оқыту процесінде анықталған салмақ коэффициенттеріне сәйкес келетін 3060642 параметрлер.

Нейрондық желі моделінің әзірленген негізгі нұсқасы Attention механизмін қамтымайтынын ескереміз, өйткені теориялық зерттеулердің нәтижелері оны CNN нейрондық желіге сәйкес келетін модульде де, RNN желіге сәйкес келетін модульде де пайдалану мүмкіндігін көрсетеді. Сонымен қатар, оны қол жетімді

әдебиеттерде интегралды нейрондық желі моделінің құрылымына енгізудің орындылығы туралы сынақтан өткен формальды шешімдер табылған жоқ.

Сондықтан Attention механизмін пайдалану негізгі интегралды нейрондық желі моделін құрудан асып түседі және оны аталған модельді өзгерту кезінде негіздеуге болады.

Сондай-ақ ұсынылған интегралды нейрондық желі моделінің модификацияланған нұсқаларында 64x64 моделінің CNN нейрондық желісінің кіріс өрісін 0,2-ден 2-ге дейінгі диапазонда сыналған біркелкі масштабтау механизмін және графикалық материалдардың пропорцияларын шамамен 20-30% өзгертуге мүмкіндік беретін сыналған біркелкі емес масштабтау механизмін пайдалану мүмкіндіктерін ескере отырып, талданатын графикалық материалдар өлшемдерінің өзгергіштігіне бейімдеу мүмкіндігін қарастыру қажет.

Осылайша, жүргізілген зерттеулер нәтижесінде онлайн-әлеуметтік желілердің графикалық материалдарындағы саяси экстремизмді тануға арналған нейрондық модельдің негізгі нұсқасы жасалды, ол өзінің CNN және RNN нейрондық желілерінің құрылымын құрайтын архитектуралық параметрлерге негізделгенін анықтау арқылы танудың тиісті тиімді әдісін жасауға мүмкіндік береді. Сонымен қатар, ұсынылған нейрондық желі моделін жетілдіру жолдарын кіріс өрісін онлайн әлеуметтік желілердегі графикалық материалдар өлшемдерінің өзгергіштігіне бейімдеумен, модельді Attention механизмін қолдануға бейімдеумен, сондай-ақ қайталанатын және толық байланысқан қабаттардың параметрлерін нақтылаумен байланыстырған жөн. Көрсетілген параметрлерге мыналар жатады: қайталанатын қабат түрі, қайталанатын қабаттар саны, қайталанатын қабаттардың әрқайсысындағы жасушалар саны, толық байланысқан қабаттар саны және толық байланысқан қабаттардың әрқайсысындағы нейрондар саны. Бұл параметрлерді анықтау механизмін онлайн әлеуметтік желілердің графикалық материалдарындағы саяси экстремизмді тану әдісінде қарастырған жөн деп болжануда.

3 ОНЛАЙН ӘЛЕУМЕТТІК ЖЕЛІЛЕРІНДЕ САЯСИ ЭКСТРЕМИСТІК МАЗМҰНДЫ АНЫҚТАУ ӘДІСТЕРІ

3.1 Әлеуметтік желілерінде саяси экстремизмді анықтауға арналған мәтіндер корпусын құру процедурасы

Мәтіндік ресурсты алуға дайындық кезеңі.

Бастапқыда, үлкен көлемді ақпараттың қажеттілігіне байланысты «Youtube», «ВКонтакте», «Telegram» секілді әлеуметтік желілерден мәтіндік және графикалық ресурстар жинақталды. Әлеуметтік желілеріндегі саяси экстремистік мәтіндерді анықтау мақсатында ең алдымен үлкен көлемдегі қазақ тілінде саяси экстремистік бағыттағы мәтіндік корпус қажет болды. Аталған корпус мәтіндері машиналық оқыту алгоритмдерін үйрету және тестілеу кезеңдерінде қолданылады. Бастапқыда ашық, қол жетімді әлеуметтік желі ресурстарынан экстремистік мәтіндер іздестірілді. Өкінішке орай ондай дайын корпустың болмауына байланысты, аталған әлеуметтік желілерден шамамен 300 – ден аса топтардан 4000 – нан аса мәтіндер жинақталып, корпусқа ендірілді. Мәтіндерді әлеуметтік желілерден жинау мақсатында парсер программалары қолданылған болатын. Бірінші, парсер модулінің кірісіне мәтіндері жүктелуі керек болатын топтардың тізімдерін беру қажет. Әлеуметтік желідегі парсинг жасалатын топтар тізімі ашық дереккөздердегі экстремистік мәтіндерге TF-IDF әдісін қолдану арқылы анықталған кілттік сөздер көмегімен құрылды. Атап айтатын болсақ, әлеуметтік желі топтарын анықтау үшін "митинг", "революция", "ұяшық", "соғыс" және т.б. сөздер қолданылды.

Зерттеу жұмысы барысында жинақталған корпусқа саяси экстремистік мәтіндермен қатар бейтарап мазмұндағы мәтіндерді жинау да жоспарланды. Саяси экстремистік мазмұндағы мәтін ретінде экстремистік іс – әрекеттерді насихаттайтын, оны орындауға шақыратын, саяси экстремистік ұйымдардың іс – әрекетін қаржыландыруға шақыруды, ұяшықтар құруға қызығушылық танытатын және т.б. қамтитын мәтіндер таңдалды.

Зерттеу жұмысы барысында Қазақстан Республикасының территориясында таратуға тыйым салынған бірнеше топтар анықталды. Олардың қатарына «ДВК», «Көше партиясы» және т.б. жатқызуға болады.

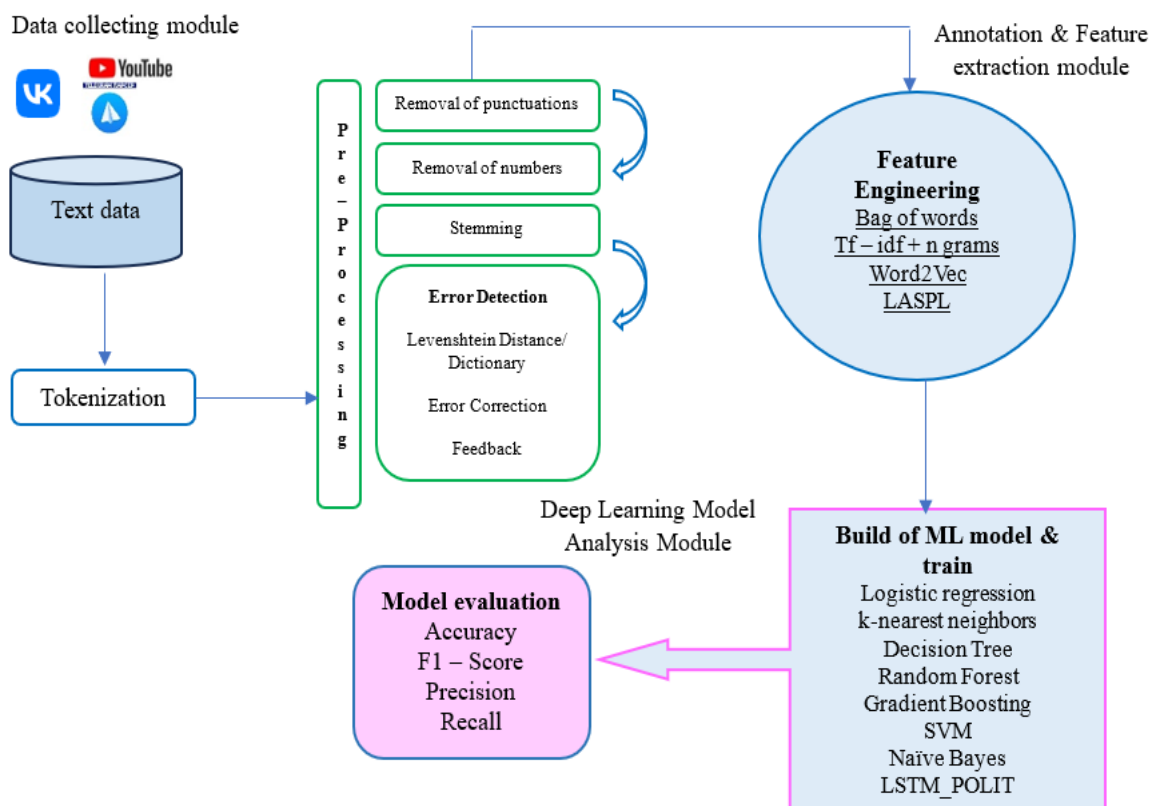
Мәліметтерді жинақтау.

Ақпаратты саяси экстремистік категорияға жатқызбас бұрын, "қауіп" критерийін анықтау қажет. Шешімдердің бірі – кілт сөздер жиынтығын анықтау. Өзірленген бағдарламалық кешенде ақпарат түрлерін анықтаудың дәл осы әдісі қолданылды. Әлеуметтік желісіндегі ақпаратты талдау үшін қолданылатын кілт сөздер жиынтығы жасалды. Бағдарламалық кешен мәтінде көрсетілген кілт сөздердің болуы немесе болмауына негізделі, мәтінде одан әрі зерттеу керекпе немесе керек емеспе деген қорытынды жасайды [60, 61, 62].

Ұсынылған архитектура бірнеше модульдан тұрады (сурет 3.1):

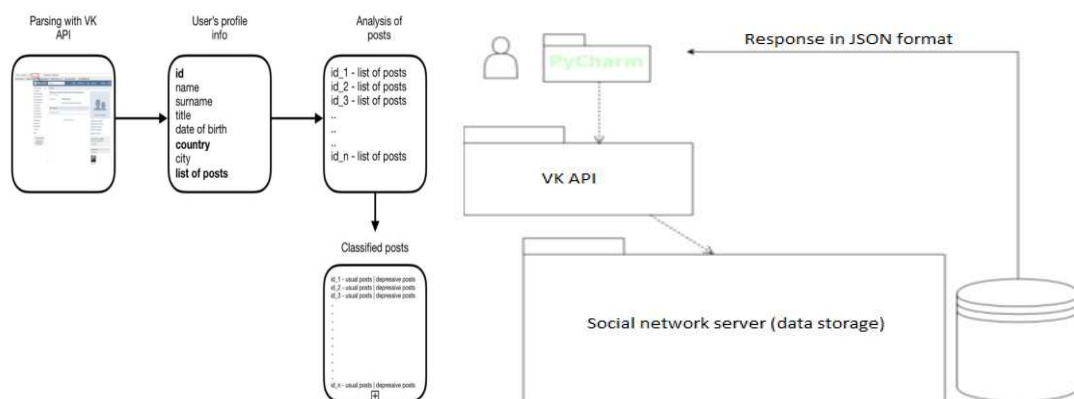
- Data collecting module (мәліметтерді алу және препроцессинг модулі);

- Annotation and feature extraction module (белгілерді шығару және мәліметтерді белгілеу модулі);
- Deep learning Model Analysis module (терең оқыту үлгілері арқылы талдау жүргізу модулі).



Сурет 3.1 – Ұсынылған архитектура

Жоғары өнімділікке қол жеткізу мақсатында ақпарат көздерінен (API) ақпарат алудың кіріктірілген әдістерін қолдану қажет. Егер мұндай әдістер болмаса, гиперсілтемелік сұраныстар арқылы қажетті ақпаратты алу қажет.



Сурет 3. 2 – Хабарламалар туралы мәліметтерді жинау, талдау және жіктеу сұлбасы

Программалық кешен 3 бөлек модульден құралады:

1) Data collection module — жинақталған мәліметтерді қабылдағаннан кейін өңдеу процессіне жауап береді;

2) Keyword search module – жинақталған үлкен көлемді ақпарат ішінен кілт сөздерді іздеуге жауап береді;

3) Data select module – жинақталған ақпараттың қауіпті екендігін анықтайды. Жинақталған мәтіндік ресурстардың қауіптілік дәрежесін анықтау үшін Long Short Term Memory (LSTM) терең оқыту алгоритмі қолданылды.

Мәліметтерді жинақтау, талдау және т.б. процестер үшін Python программалу тілі қолданылды.

Әлеуметтік желінің API – мен өзара әрекеттесуі сұрау кітапханасы арқылы жүзеге асырылды. Pycharm Community Edition 2018 программалық кешені құрастыру ортасы ретінде таңдалды. Мәліметтерді алу үшін «ВКонтакте» API - ді қолданылады – серверге HTTPS сұрауларын қолдана отырып, «ВКонтакте» әлеуметтік желісінің мәліметтер қорынан қажетті ақпаратты алуға мүмкіндік беретін дайын интерфейс. Кесте 3.1 – де пайдаланушының қарапайым сұраныс компоненттері көрсетілген:

Кесте 3.1 – Сұраныс компоненттері

| Сұраныс параметрі | Түсіндірмесі |
|-------------------------------|--|
| 1 | 2 |
| <i>https: //</i> | Қосылу хаттамасы |
| <i>api.vk.com/method</i> | API қызметінің api.vk.com/method қолданушысы |
| <i>.get</i> | API V Kontakte әдісінің атауы |
| ?user_id=210700286&v=5 .92 | Сұраныс компоненті |

Әдістер – бұл белгілі бір дерекқор операциясына сәйкес келетін шартты командалар. Мысалы, пользователи.get – бұл пайдаланушылар, есептік жазба туралы ақпарат алу әдісі, getinfo ағымдағы пайдаланушы туралы ақпаратты және т. б. қайтарады. Жүйедегі барлық әдістер бөлімдерге бөлінген. Жіберілген сұрауда әдіс атауынан кейін HTTP сұрауында GET параметрлері ретінде кіріс деректерін беру керек. Егер сұраныс сәтті өнделсе, сервер сұралған деректермен JSON нысанын қайтарады. Деректерді талдау үшін pandas, numpy, matplotlib, plotly, bokeh, cufflinks, spacy, googletrans пакеттері бар Python 3.7 программалау тілі есептеу және визуализацияның негізгі кітапханалары ретінде қолданылды. Тиісті мәтіндерді іздеу үшін экстремизммен байланысты кілт сөздер анықталды. Мысалы, "кафир", "өлтіру", "жару" және т.б. бұл кілт сөздер әлеуметтік желілердегі экстремистік посттарды табуға көмектеседі. Экстремистік посттар табылған сайын, кілт сөздер базасы толықтырылып, экстремистік посттардың нақты анықтамасын қамтамасыз етеді. Мәліметтердің аннотациясы үшін «ВКонтакте» әлеуметтік желісінен экстремистік идеялардың мәтіндері жиналды

және олардың дұрыс таңбаланғанына көз жеткізу үшін барлық хабарламалар қолмен тексерілді. Аннотация ережелері мен хабарлама мысалдары 3.2 - кестеде келтірілген.

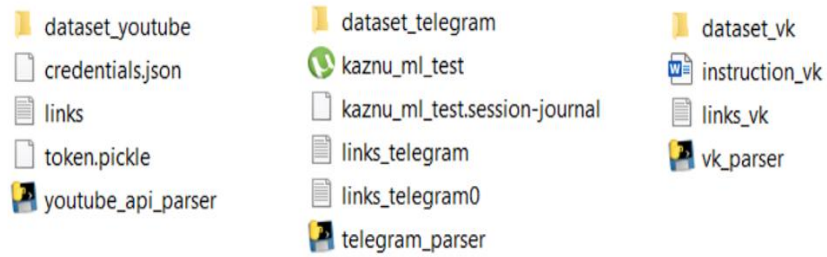
Кесте 3.2 – Аннотация ережесі

| Санаттар | Ережелер | Мысалдар |
|--------------------------|---|---|
| Саяси экстремистік мәтін | 1 деңгей Саяси экстремистік мәлімдемелер | Мен елде төңкеріс жасау дұрыс деп ойлаймын. / Я считаю правильным совершить революцию в стране. |
| | 2 деңгей Саяси экстремистік іс-әрекеттер | Мен ДВК ұйымына митингке қатысу үшін тіркелдім. / Я зарегистрировался в организацию ДВК для участия в митинге. |
| Бейтарап мәтін | 1 деңгей Саяси экстремизмді талқылау | Рұқсатсыз митинг ұйымдастырушылар көбейіп барады. / Организаторов митингов без разрешения становится все больше. |
| | 2 деңгей Басқа біреудің экстремистік талқылауына сілтеме | Құзіреттік ұйым мұның экстремистік ұйым мекендігін айтты. / В компетентной организации заявили, что это экстремистская организация. |
| | 3 деңгей Саяси экстремизмге қатысы жоқ | Бүгін ауа – райы керемет. / Сегодня чудесная погода. |

Мәліметтерді жинау үшін парсер құрастыру

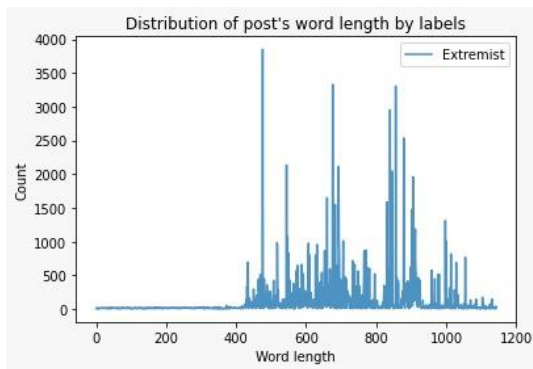
Зерттеу барысында үлкен көлемдегі деректер қажет. Қазақ тілінде дайын экстремистік корпус болмағандықтан, «ВКонтакте», «YouTube», «Telegram» және т.б. ашық ақпарат көздерінен мәлімет жинақтауға арналған парсер программасы жазылды. Парсердің нәтижесін көрсету үшін шағын веб-қосымша құрылды. 3.3 – суретте деректерді жинауға арналған парсер программасы көрсетілген.

Нәтижесінде, әзірленген парсер көмегімен экстремистік бағыттағы мәліметтер жиналды. Жіктеу модельдерін одан әрі оқыту үшін корпус әзірленді, ол "экстремистік" және "бейтарап" бағыт ретіндегі екі класстан тұрады.

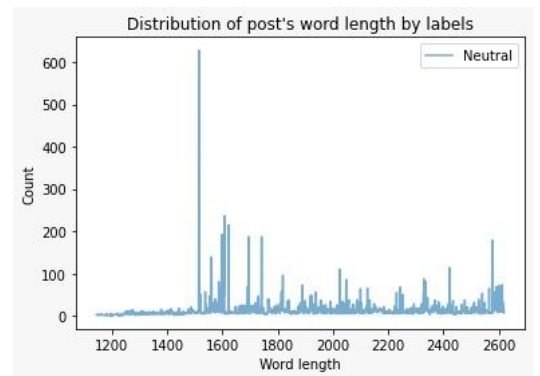


Сурет 3.3 – Әлеуметтік желілерден деректерді жинақтауға арналған парсер программалар

Корпус талдауы. Сурет 3.4 – те деректер жиынтығындағы экстремистік және бейтарап мәтіндердің үлестірімі көрсетілген.



а) Экстремистік хабарламалардың үлестірім графигі



б) Бейтарап мәтіндердің үлестірім графигі

Сурет 3.4 – Корпустағы экстремистік және бейтарап мәтіндердің ұзындықтары бойынша үлестірім кестесі

Сөздер бұлты. Деректерді визуалды түрде көрсету үшін сөз бұлттары қолданылды. Ықтимал экстремистік идеялары бар пайдаланушылардың хабарламалары сурет 3.5 – те бөлек көрсетілген.



а) Экстремистік санаттағы жиі кездесетін сөздер бұлты



б) Бейтарап санаттағы жиі кездесетін сөздер бұлты

Сурет 3.5 – Экстремистік және бейтарап санаттағы сөздер бұлты

Экстремистік мәтіндердің ерекшеліктері

Қазақ тіліндегі экстремистік мәтіндерді талдау олардың кейбір ерекшеліктерін анықтады:

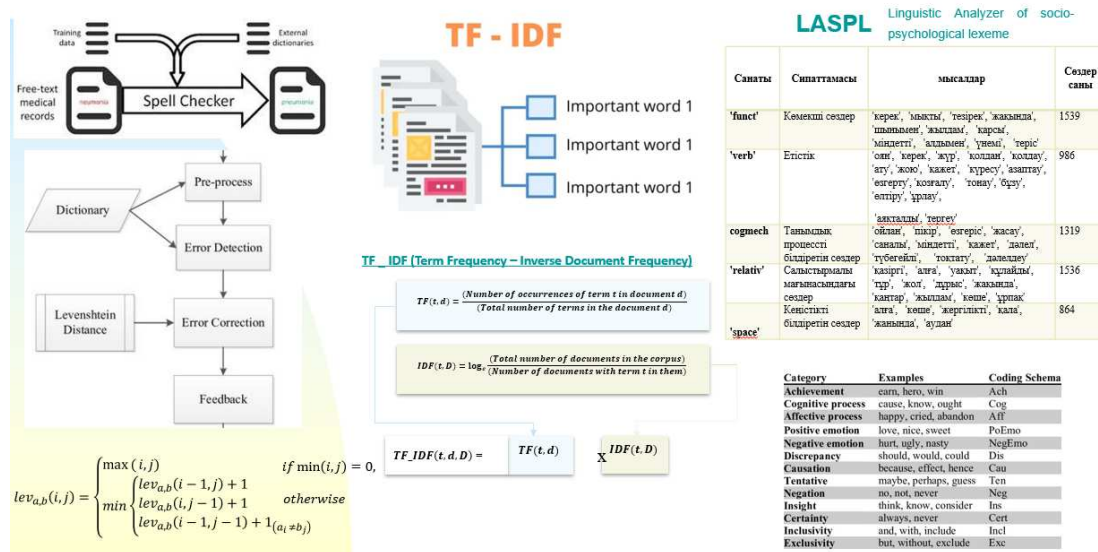
- 1) қазақ тілінің бастапқы әріптерін кириллица әріптерімен ауыстыру (мысалы, "ұяшық" сөзінің орнына "уяшык", "құрту" орнына "курту" және т. б.),
- 2) биграммаларды жиі пайдалану (мысалы, "билік құлату" және т. б.),
- 3) бір сөздің бірнеше емлесінің болуы (мысалы, "ұяшық", "уя", "ұяшк", "ұйашык", "үяшык"),
- 5) корпустағы жиі орфографиялық қателер (грамматикалық қателер емес, теру кезінде пайда болатын қателер).

Алынған нәтижелер. Осы тараудың нәтижесінде,

- а) парсер программалардың көмегімен «Youtube», «ВКонтакте», «Telegram» секілді әлеуметтік желілерден мәтіндік және графикалық ресурстар жинақталды;
- б) мәтіндерді "экстремистік" және "бейтарап" деп танылған екі санатқа жіктелді;
- в) модельді одан әрі оқыту мақсатында корпус құрылды;
- г) экстремистік және бейтарап сипаттағы мәтіндерді, сөз бұлтын бөлу арқылы корпуста талдау жүргізілді және экстремистік мазмұндағы мәтіндердің ерекшеліктері анықталды.

3.2 Онлайн әлеуметтік желілеріндегі саяси мазмұнды мәтіндік материалдарды анықтау әдісі

Бұл бөлімде терең оқыту алгоритмдері көмегімен табиғи тілді өңдеу әдістеріне (3.6-сурет) сипаттама беріледі. Мұндай әдістерге Spell Checker, TF – IDF, LASPL және т.б. жатады.



Сурет 3.6 – LSTM желісінің кіріс қабатын қалыптастыру әдісі

Айта кету керек, орфографиялық қателерді түзету қиын жұмыс, әсіресе сөздің екіұштылығы бар немесе бір мағыналы дұрыс жазылуы жоқ жағдайларда. Орфографиялық қателерді түзету кезінде мәтіннің контексті мен мағынасын да ескеру қажет.

Spell checker - емлені тексеруді және қатені түзетуді жүзеге асыратын құрал. Ол бірнеше тілді қолдайды. Ол Python программалау тілімен үйлесімді. Бұл құрал ашық бастапқы болып табылады және Левенштейн қашықтығы принципіне негізделген. Ол бастапқы сөзден 2 өңдеу қашықтығында болатын ықтимал ауыстыруларды таба алады. Левенштейн қашықтығы немесе өңдеу қашықтығы ретінде белгілі, екі жол арасындағы айырмашылықты өлшеу үшін пайдаланылатын метрика. Ол бір жолды екіншісіне түрлендіру үшін қажетті әрекеттердің (енгізулер, жоюлар және ауыстырулар) ең аз санын көрсетеді. Левенштейн қашықтығы емле қателерін түзету, мәтіндердің ұқсастығын анықтау, тізбектерді салыстыру және т.б. сияқты көптеген мәтінді өңдеу тапсырмаларында пайдалы. Ол екі жолдың ұқсас немесе әртүрлі екенін бағалауға мүмкіндік береді, яғни ол барлық ауыстыруларды сөз жиілігі тізіміндегі белгілі сөздермен салыстырады. Бұл тізімде жиі кездесетін сөздер дұрыс нәтижелер болуы ықтимал [63, 64].

Левенштейн қашықтығын есептеу формуласы динамикалық бағдарламалауға негізделген және аралық мәндерді сақтау үшін матрицаны пайдаланады.

Мысалы, сурет 3.7 – де сәйкесінше Левенштейн бойынша бір ауыстыру және екі жою қажет болады:

| | | | |
|---|---|---|---|
| Б | И | Б | А |
| Б | О | Б | А |

а)

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| А | В | С | Т | Р | | | И | Я |
| А | В | С | Т | Р | А | Л | И | Я |

ә)

Сурет 3.7 – Левенштейн қашықтығына мысал

Spell checker алгоритмі күтілетін емле үлгілеріне сәйкес келмейтін сөздерді анықтау үшін берілген мәтіндегі сөздерді сөздікпен немесе тіл үлгісімен салыстырады. Олар мәтіннің дәлдігін жақсарту үшін балама емлелерді ұсынады немесе түзету опцияларын ұсынады.

Орнатудың ең оңай жолы pip пайдалану: `pip install pySpell checker`

Төмендегі кесте 3.3 – те сипатталған функциялар мәтінді өңдеуге арналған кейбір қолжетімді әдістер немесе функциялар туралы ескертпелер:

Кесте 3.3 – Мәтінді өңдеудегі әдістер

| | |
|------------------------|--|
| correction(word) | Қате жазылған сөз үшін ең ықтимал түзетуді қайтарады. Ол тілдік модельге және мәтіндегі сөздердің кездесу ықтималдығына негізделген. |
| candidates(word) | Қате жазылған сөз үшін ықтимал түзету үміткерлерінің жинағын қайтарады. Ол айналадағы мәтінмәнді талдап, емле немесе дыбыс жағынан ұқсас болуы мүмкін нұсқаларды ұсынады. |
| known([words]) | Функция жиілік сөздігінде немесе белгілі сөздер тізімінде бұрыннан бар тізімдегі сөздердің ішкі жиынын қайтарады. Бұл мәтінді сүзу немесе сөздердің жиілігін анықтау кезінде пайдалы. |
| unknown([words]) | Жиілік сөздігінде немесе белгілі сөздер тізімінде бұрыннан бар тізімдегі сөздердің ішкі жиынын қайтарады. |
| word_probability(word) | Берілген сөздің жиілік сөздігіндегі немесе тізімдегі барлық сөздердің арасында пайда болу ықтималдығын есептейді. Оны мәтіндегі сөздің маңыздылығын немесе таралуын бағалау үшін пайдалануға болады. |

Бұл мәтінді өңдеу мүмкіндіктерін қателерді түзету, баламаларды ұсыну, мәтінді сүзу немесе сөз жиілігін анықтау үшін пайдалануға болады. Олар мәтінмен жұмыс істеу процесін автоматтандыруға және жақсартуға және талдау мен өңдеудің дәлдігін жақсартуға көмектеседі.

Қылмыстық мәтіндерді анықтау тапсырмаларында емле қателерін түзету кезінде мәтіннің контексті мен мағынасын ескеру маңызды. Дұрыс емес түзету мәтіннің мағынасының бұрмалануына және қате жіктелуіне әкелуі мүмкін.

Spell checker қазақ тілін қолдамайтындықтан, сондағы әдіс Ливенштейн қашықтығын қолдана отырып, қазақ тіліндегі сөздердің орфографиялық қатесін түзейтін функция құрылды.

Бірінші қазақ тіліндегі мәтіндер жинағы жасалынған, read_corpus() функциясы сондағы мәтіндік файлды ашады, оның мазмұнын оқиды және сөздер тізімін береді. Сурет 3.8 – де сипатталған edit_distance() функциясы екі сөз арасындағы Левенштейн қашықтықты есептеу алгоритмін жүзеге асырады, ал corrector() функциясы сөйлем мен сөздікті алып, сөйлемді бөлек сөздерге бөледі және әрбір сөз үшін оның сөздікте болуын тексереді.

```

def edit_distance(word1, word2):
    m = len(word1)
    n = len(word2)
    dp = np.zeros((m + 1, n + 1))
    for i in range(m + 1):
        dp[i, 0] = i
    for j in range(n + 1):
        dp[0, j] = j
    for i in range(1, m + 1):
        for j in range(1, n + 1):
            if word1[i - 1] == word2[j - 1]:
                dp[i, j] = dp[i - 1, j - 1]
            else:
                dp[i, j] = min(dp[i - 1, j], dp[i, j - 1], dp[i - 1, j - 1]) + 1
    return dp[m, n]

def corrector(sentence, vocabulary):
    words = sentence.split()
    corrected_sentence = []
    print(words)
    for word in words:
        if word in vocabulary:
            corrected_sentence.append(word)
        else:
            suggestions = []
            for candidate in vocabulary:
                if abs(len(candidate) - len(word)) > 1:
                    continue
                distance = edit_distance(candidate, word)
                if distance <= 1:
                    suggestions.append(candidate)

            if suggestions:
                corrected_sentence.append(suggestions[0])
            else:
                corrected_sentence.append(word)

    corrected_sentence = " ".join(corrected_sentence)
    return corrected_sentence

```

Сурет 3.8 – Емле түзету бойынша функциялар коды

Код бойынша алдымен сөйлемдегі әрбір сөздің сөздікте болуын тексереді. Егер сөз бұрыннан сөздікте болса, ол түзетілген сөйлемге өзгеріссіз қосылады. Егер сөз сөздікте табылмаса, функция бұрынғыдай Левенштейн қашықтығы арқылы ұсынылған түзетулерді іздейді. Содан кейін ол бірінші ұсынылған түзетуді таңдап, оны түзетілген ұсынысқа қосады. Егер сөзге ұсынылған түзетулер табылмаса, өзгеріссіз қалады.

| message | corrected |
|---|---|
| алға двк алға мұхтар аблязов наш будиший приме... | ала двк ала мұхтар әблязов наш бадий премьер ... |
| оян қазақ ойлан қазақ билікте отырған ұры қара... | оян қазақ ойлан қазақ билікте отырған ұры сара... |
| қазіргі биліктегі отырған ұры қарақшы жемқор а... | қазіргі биліктегі отырған ұры қармақшы қамқор ... |
| алға двк мұхтао ағамызды колдайық колдарыңызжа... | ала двк мұхтар ағамыздың колдайық колдарыңызжа... |
| двк программасымен өзгеріске алға двк программ... | двк программасын өзгеріске алға двк программас... |

Сурет 3.9 – Емле түзету функциясының нәтижесі

TF - IDF. Мәтіндік деректерді сандарға ауыстыру қажет және мәтіндік деректерді сандарға өңдеудің кең қолданылатын әдісі – TF-IDF болып табылады. TF-IDF-де мәтіндік мәліметтер векторларға айналады, олар сөздердің реттілігінің нақты дәйектілігін ескермейді. Корпустағы әрбір сөз TF-IDF санымен байланысты, бұл әр сөздің корпус үшін қаншалықты маңызды екендігін көрсетеді [65].

Сөздерді сандарға айналдырғаннан кейін, TF-IDF сандық мәндері машиналық оқыту әдістері түсіндіре алатын контекстте бақыланатын оқыту жіктеуіштеріне беріледі.

TF-IDF – құжаттағы терминдердің өлшемді векторлық көрінісі. Ол құжатта пайда болған әр терминге салыстырмалы салмақты терминнің дифференциалдау қабілеттілігіне сәйкес тағайындайды, бұл құжатқа тиісті белгіні тағайындауға көмектеседі. TF-IDF бойынша, егер термин корпустағы барлық құжаттарда пайда болса, онда ол онша маңызды емес және оған аз салмақ беру керек, екінші жағынан салыстырмалы түрде аз құжаттарда пайда болса, оған үлкен салмақ беру керек деп есептеледі.

TF (term frequency — сөз жиілігі) — қандай да бір сөздің құжатта кездесуінің құжаттағы барлық сөздер санына қатынасы. t сөзінің жеке құжат шеңберіндегі маңыздылығы есептеледі.

$$tf(t, d) = \frac{n_t}{\sum_k n_k} \quad (3.1)$$

Мұндағы n_t – t сөзінің құжатта кездесу саны, ал бөлімінде берілген құжаттағы сөздердің жалпы саны.

IDF (inverse document frequency — құжаттың кері жиілігі) — қандай да бір сөздің жинақ құжаттарында кездесу жиілігінің инверсиясы. IDF кең қолданылатын сөздердің салмағын азайтады. Нақты бір құжаттар жинағындағы әрбір бірегей сөз үшін бір ғана IDF мәні болады.

$$idf(t, D) = \log \frac{|D|}{|\{d_i \in D \mid t \in d_i\}|} \quad (3.2)$$

Мұндағы $|D|$ - жинақтағы құжаттар саны, $|\{d_i \in D \mid t \in d_i\}|$ - D жинағындағы t кездесетін құжаттар саны ($n_t \neq 0$).

TF-IDF өлшемі екі шаманың көбейтіндісі түрінде есептеледі:

$$tf - idf(t, d, D) = tf(t, d) * idf(t, D) \quad (3.3)$$

n-грамдар. Берілген жұмыста қолданылған тағы бір белгі – n -грамдық ендіру әдісі. n -грам тиімді техника болып табылады, өйткені ол корпустағы сөздер ретін ұсынады.

N -gram – символдар немесе сөздер қатарынан тұратын токен. Токен мәтіндер корпусы бойымен сырғымалы терезені жылжыту арқылы қалыптасады, терезенің өлшемі токеннің өлшеміне байланысты, ал жылжыту кезең бойынша орындалады, әр кезең сөзге немесе символға сәйкес келеді.

:ұмыста n -грам бірнеше сөздің тізбегі ретінде анықталған: 1 грам (униграмма), 2 грам немесе биграмма – екі сөзден құралған тізбек, ал 3 сөз немесе триграмма – үш сөзден құралған тізбек.

Мәтіндік деректерді салмақталған векторға айналдыру және хабарламадағы сөз тізбегіне ықтималдықтарды тиімді бөлу үшін n -граммдық модель қолданылады. N -грамм моделін түсіну үшін хабарламаны мысал ретінде келтірейік, мысалы: «Менің әпкем ауырып жатыр, ол тезірек сауығып кетеді деп

үміттенемін'». Биграммдық n-граммдық интерпретациясы (бұл жағдай үшін $N - 1 = 1$, сөздің пайда болуын алдыңғы сөзге сүйене отырып болжайды) «менің әпкем», «әпкем ауырып», «ауырып жатыр», «жатыр ол», «ол тезірек», «тезірек сауығып», «сауығып кетеді», «кетеді деп», «деп үміттенемін» түрінде болады.

d_1 және d_2 құжаттарының ұқсастығын олардың n-gram түрінде ұсынулары $S_n(d_1)$ және $S_n(d_2)$ арқылы анықтауға арналған Жаккард коэффициенті келесі теңдеуде келтірілген:

$$\text{sim}(d_1, d_2) = \frac{|S_n(d_1) \cap S_n(d_2)|}{|S_n(d_1) \cup S_n(d_2)|} \quad (3.4)$$

d_1 және d_2 құжаттары бір-бірінің көшірмесі екендігін анықтау үшін шектік мән пайдаланылады. Әрбір қосымша үшін терезенің өлшемі мен ұқсастық шегі тәжірибелер барысында таңдалады.

жұмыста n-грам негізіндегі модельді n-грамнің тілдегі ықтималдығын болжау үшін пайдаланылатын ықтималдық моделі деп атаған. Берілген ықтималдықтар негізінде d құжатының белгілі бір c классына тиіс екендігін анықтауға болады:

$$P(c|d) = \prod_{i=1}^n P(w_i | w_{i-n+1}^{i-1}) \quad (3.5)$$

$$P(w_i | w_{i-n+1}^{i-1}) = \frac{\text{freq}(w_{i-n+1}^{i-1} w_i)}{\text{freq}(w_{i-n+1}^{i-1})} \quad (3.6)$$

мұндағы freq - n-gram-ның класстағы жиілігін білдіреді.

LASPL (Linguistic Analyzer of socio-psychological lexeme). Келесі әдіс - қазақ тіліндегі саяси экстремистік мазмұнды қамтитын мәтіндердегі лексемаларға психо-эмоционалдық талдау модулі әзірленді. Зертеу жұмысы барысында сөздерді санау стратегиясын және liwc жабық сөздік әдісін қолдана отырып, саяси экстремистік лингвистикалық корпусы талданады. Ұсынылатын әдістің міндеті - мәтіндік деректер жиынтығында психологиялық категорияларға қатысты сөздерді іздеу және санау. Барлығы 80 –нен артық санат бөлінді. Бағдарламада мәтіндік файлды өңдеудің нәтижесі келесі шығыс айнымалылары болып табылады: сөздер саны, жиынтық тілдік айнымалылар (аналитикалық ойлау, әсер ету, мәтіннің өзіндік ерекшелігі және эмоционалды тон) және мәтіндегі сөздердің пайызын көрсететін тілдік өлшем (мысалы, есімдіктер, мақалалар, көмекші етістіктер және т. б. болып табылатын мәтіндегі сөздердің пайызы. д.), психологиялық құрылымдарға әсер ететін санаттар (мысалы, аффект, таным, биологиялық процестер, импульстар), жеке қызығушылық санаты (мысалы, жұмыс, үй, демалыс), бейресми тіл маркерлері (мысалы, қарғыс). Нәтижелер сөздерді қолдану тәсілдерінде тұлғаның даму деңгейлерінің көрінісі туралы жалпы теориялық білімнің пайдасын көрсетеді [66].

Кесте 3.4 – Мәтіндердегі лексемаларға психо-эмоционалдық талдау модулі

| Категория | Сипаттама | Мысалдар | Категориядағы табылған сөздер саны |
|-------------|--------------------------------------|---|------------------------------------|
| 'funct' | Көмекші сөздер | 'керек', 'мықты', 'тезірек', 'жақында', 'шынымен', 'жылдам', 'қарсы', 'міндетті', 'алдымен', 'үнемі', 'теріс' | 1539 |
| 'verb' | Етістік | 'оян', 'керек', 'жүр', 'қолдан', 'қолдау', 'ату', 'жою', 'қажет', 'күресу', 'азаптау', 'өзгерту', 'қозғалу', 'тонау', 'бұзу', 'өлтіру', 'ұрлау', 'аяқталды', 'тергеу' | 986 |
| 'affect' | Әсер ету мағынасындағы сөздер | 'ұры', 'күрес', 'ату', 'белсенді', 'өтірік', 'жою', 'қауіп', 'оңбаған', 'қару', 'зұлым', 'бағынышты', 'наразылық', 'қысым', 'қызмет', 'сыйақы', 'зардап', 'көтеріліс', 'қорқынышты', 'ауыр', 'жау', 'еркіндік', 'жауыз', 'дайындық' | |
| 'posemo' | Позитивті эмоцияны білдіретін сөздер | 'жақсылық', 'адал', 'сенімді', 'сәттілік', 'жеңіс', 'белсенді', 'сыйақы', 'лайықты', 'оңай', 'еркіндік', 'үміт', 'құрмет', 'жігер', 'сенім', 'бай', 'дайындық', 'мақтаныш' | |
| 'negemo' | Негативті эмоцияны білдіретін сөздер | 'ұры', 'күрес', 'ату', 'өтірік', 'қауіп', 'заңсыз', 'қару', 'дау', 'қорқақ', 'бағынышты', 'наразылық', 'қысым', 'қылмыс', 'зардап', 'көтеріліс' | |
| 'cognitive' | Танымдық процессті білдіретін сөздер | 'ойлан', 'пікір', 'өзгеріс', 'жасау', 'саналы', 'міндетті', 'қажет', 'дәлел', 'түбегейлі', 'тоқтату', 'дәлелдеу' | 1319 |
| 'relativ' | Салыстырмалы мағынасындағы сөздер | 'қазіргі', 'алға', 'уақыт', 'құлайды', 'тұр', 'жол', 'дұрыс', 'жақында', 'қаңтар', 'жылдам', 'көше', 'ұрпақ' | 1536 |
| 'motion' | Әрекетті білдіретін сөздер | 'алға', 'жүр', 'ату', 'өзгеріс', 'көтерілу', 'жою', 'қозғалыс', 'күресу', 'соғыс', 'өзгерту', 'өлтіру', 'ұрлау' | |
| 'space' | Кеңістікті білдіретін сөздер | 'алға', 'көше', 'жергілікті', 'қала', 'жанында', 'аудан' | 864 |
| 'time' | Уақытты білдіретін сөздер | 'қазіргі', 'жақында', 'кеш', 'қаңтар', 'әрқашан', 'минут', 'күні', 'желтоқсан', 'қараша', 'тамыз', 'қазан' | |

3.3 Әлеуметтік желілерінің графикалық ресурстарында саяси экстремизмді анықтау әдісі

Саяси экстремизмді анықтау әдісін әзірлеудің бастапқы нүктесі ретінде осы жұмыстың екінші бөлімінде әзірленген онлайн әлеуметтік желілердің

бейнелері мен бейнематериалдарын алдын ала өңдеу және нейрондық желіні талдау модельдері пайдаланылды.

Сонымен қатар, әдісті құру кезінде нейрондық желі моделінің кіріс өрісін онлайн әлеуметтік желілердің графикалық ресурстарының өзгергіштігіне бейімдеу қажеттілігі ескерілді. Көрсетілген алғышарттарға сәйкес аналитикалық түрде ұсынылған әдісті қолдана отырып ақпаратты өңдеуді келесі өрнектер арқылы ұсынуға болады:

$$\langle GM, M, D \rangle \rightarrow Y_{GM} \quad (4.1)$$

$$\langle G, N, Q, DS, Z, A \rangle \rightarrow D \quad (4.2)$$

мұндағы GM – онлайн әлеуметтік желінің талданатын графикалық ресурсы параметрлерінің мәндерін қамтитын кортеж; M – графикалық ресурстарды алдын-ала өңдеу моделінің параметрлерінің мәндерін қамтитын кортеж; D – кортеж, содержащий значения параметров используемой нейросетевой модели; Y_{GM} – графикалық ресурстарды нейрондық талдаудың нәтижелері бар жиын; G – талданатын онлайн әлеуметтік желінің графикалық ресурстары параметрлерінің мәндерін қамтитын кортеж; N – нейрондық желі модельдерінің қол жетімді түрлерінің параметрлерінің мәндерін қамтитын кортеж; Q – тану процесін сипаттайтын жағдайлар кортежі; DS – нейрондық желі моделінің оқу үлгісінің мысалдары бар жиын; Z – нейрондық желі модельдерін құру үшін қолданылатын көптеген сараптамалық мәліметтер; A – нейрондық желі модельдерінің тиімділігінің көптеген критерийлері.

Айта кетейік, өрнек (4.1) белгілі бір онлайн әлеуметтік желінің графикалық ресурстарын тану процесімен байланысты, ал өрнек (4.2) графикалық ресурстарды алдын ала өңдеу процедурасы мен нейрондық желі моделін құру процедурасын қамтитын тану құралдарын құру процесімен байланысты. Бұл жағдайда GM (3.2) өрнек арқылы анықталады, ал M (2.1-2.24) өрнектермен анықталады.

Негізгі жағдайда Y_{GM} осы нейрондық желі моделінің шығысымен байланыстыруға болады.

Сондай-ақ, бірінші жуықтауда нейрондық желі модельдерінің (A) тиімділігінің көптеген критерийлерінің құрамдас бөліктері A_1, A_2, A_3 , болып табылады, олар онлайн әлеуметтік желілердің графикалық ресурстарын талдаудың нейрондық желілік моделін әзірлеуге арналған бөлімде анықталған.

(4.1, 4.2) компоненттері (4.3-4.8) өрнектерінің көмегімен әзірленген.

$$G = \langle C, S \rangle, \quad (4.3)$$

$$S = \{s_1, s_2, s_3\}, \quad (4.4)$$

мұндағы C – графикалық формат GM ; S – GM өлшемі; s_1 – GM ені; s_2 – GM биіктігі; s_3 – GM кадрлар саны.

Айта кетейік, $GM = Im, s_3=1$ жағдайында.

$$N = \langle T, R_T \rangle \quad (4.5)$$

мұндағы T - (3.13) өрнектің көмегімен анықталатын CNN нейрондық

желілердің көптеген қолайлы түрлері; $R_T - T$ компоненттерінің параметрлері бар массив.

$$Q = \langle Q_1, Q_2 \rangle \quad (4.6)$$

$$Q_1 = \langle N_R, N_A \rangle \quad (4.7)$$

$$Q_2 = \langle s_{1,min}, s_{2,min}, s_{1,max}, s_{2,max}, C_{GM} \rangle \quad (4.8)$$

мұндағы Q_1 – тану құралдарына қойылатын талаптар; Q_2 – талданатын материалдардың параметрлері; N_R – тану құралдарының рұқсат етілген ресурс сыйымдылығы; N_A – рұқсат етілген тану дәлдігі; $s_{1,min}, s_{2,min}$ – талданатын әлеуметтік желінің графикалық ресурстарының ені мен биіктігінің мүмкін болатын ең төменгі мәні; $s_{1,max}, s_{2,max}$ – графикалық ресурстардың ені мен биіктігінің мүмкін болатын ең үлкен мәні; C_{GM} – талданатын әлеуметтік желідегі ресурстардың көптеген мүмкін графикалық форматтары.

Ұсынылған саяси экстремизмді анықтау процедурасының сұлбасы 3.10 – суретте көрсетілген. Аталған анықтау процедурасының кезеңдерін жүзеге асыру кезінде диссертацияның екінші бөлімінде ұсынылған модельдерді әзірлеу кезінде алынған шешімдер қолданылатынын ескереміз.

Сонымен, графикалық ресурсты алдын – ала өңдеу кезінде:

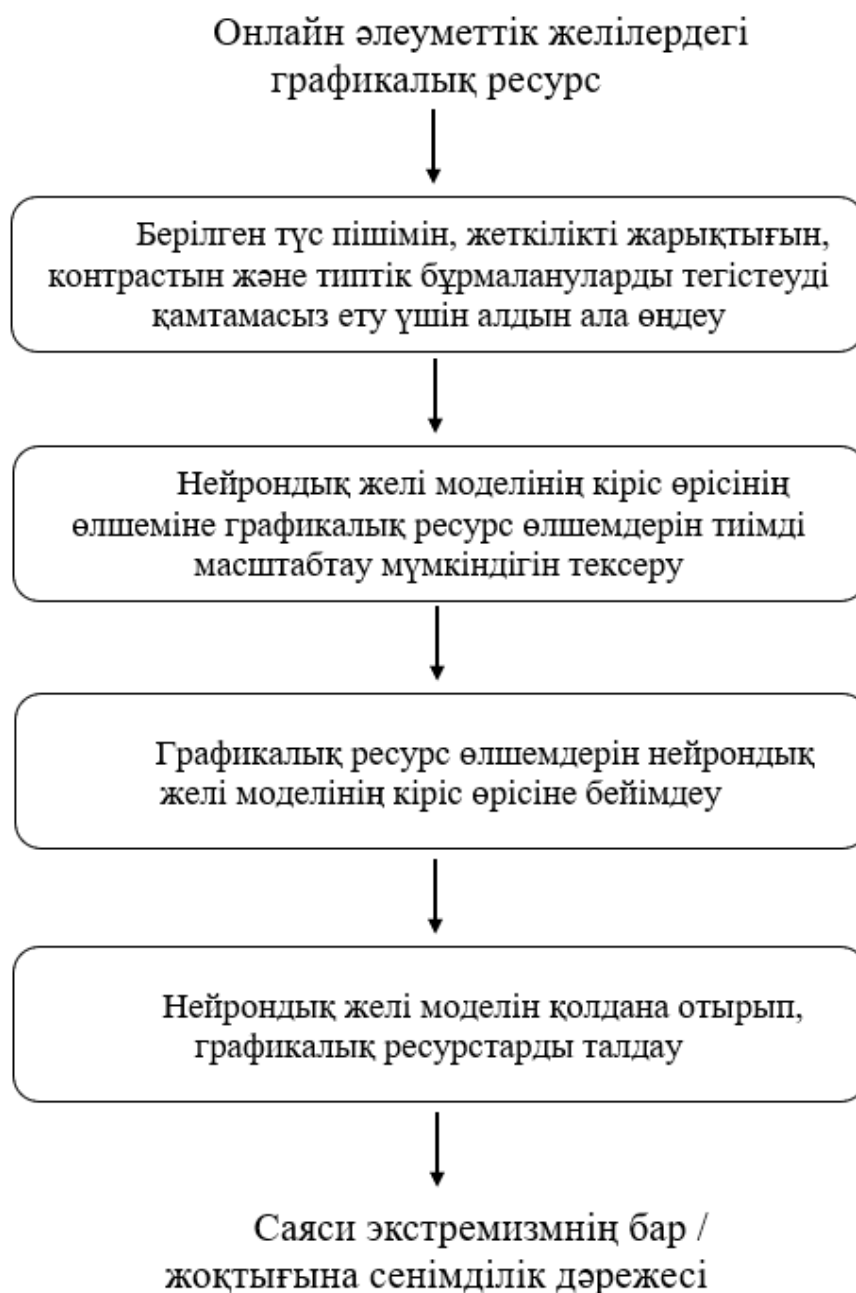
- для обеспечения заданного цветового формата с нормализованными значениями по каждому цветовому каналу – выражения (2.7-2.9), что позволяет конвертировать анализируемый многоканальный графический ресурс в полутоновый или бинарный формат и выражение (2.10), обеспечивающее нормализацию цвета каждого пикселя; әр пиксельдің түсін қалыпқа келтіруді қамтамасыз етуде әрбір түс арнасы бойынша нормаланған мәндермен берілген түс форматын қамтамасыз ету үшін (2.7-2.9) өрнектері, талданатын көп арналы графикалық ресурсты жартылай тонға немесе екілік форматқа түрлендіруге (2.10) өрнегі мүмкіндік береді;
- түс арналарының жарықтығын түзету үшін (2.11, 2.12) өрнектері;
- контрастты түзету үшін (2.13-2.16) өрнектері;
- $k_{max} = 0,9$, $k_{min} = 0,2$, $a = 0,6$, $d = 20$ негізге ала отырып, типтік бұрмалануларды түзету үшін (2.17-2.24) өрнектері.

Сонымен қатар, графикалық ресурстарды өңдеу моделінде қарастырылған типтік кедергілерді жою процедурасын жүзеге асыру үшін жұмыста ұсынылған эталонсыз механизмді қолдана отырып, кескін сапасын бағалау механизмін қолдану ұсынылады.

Эталонсыз бағалау механизмін қолдану оқу мысалдарының дерекқоры қалыптасқан жағдайда да, онлайн әлеуметтік желілердің графикалық ресурстарын нейрондық желілік талдау жағдайында да анықтамалық кескін көбінесе қол жетімді емес екендігімен түсіндіріледі.

Кескін сапасын анықтау үшін нәтижелерінде Tenengrad деп аталатын әдіс пайдаланылды. Ол жеткілікті дәлдікпен және есептеулердің аздығымен ерекшеленеді, онлайн режимінде әлеуметтік желілердегі саяси экстремизмді анықтау жүйелерінде пайдалануға мүмкіндік береді. Tenengrad әдісі талданатын

кескіннің сәйкес түрленуін болжайтын жартылай реңкті кескіннің пиксель жарықтығы градиентінің орташа квадратын бағалауға негізделген. Кескінді ең көп таралған RGB форматынан түрлендіру үшін (2.7) өрнегі қолданылады.



Сурет 3.10 – Саяси экстремизмді анықтау процедурасының сұлбасы

Тененград әдісін енгізу келесі өрнектермен сипатталады:

$$S_{S_1}(x, y) = \begin{vmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{vmatrix} * A(x, y), \quad (4.9)$$

$$S_{s_2}(x, y) = \begin{vmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{vmatrix} * A(x, y), \quad (4.10)$$

$$S = \sum_{x=1}^{s_1} \sum_{y=1}^{s_2} (S_{s_1}(x, y)^2 + S_{s_2}(x, y)^2), \quad (4.11)$$

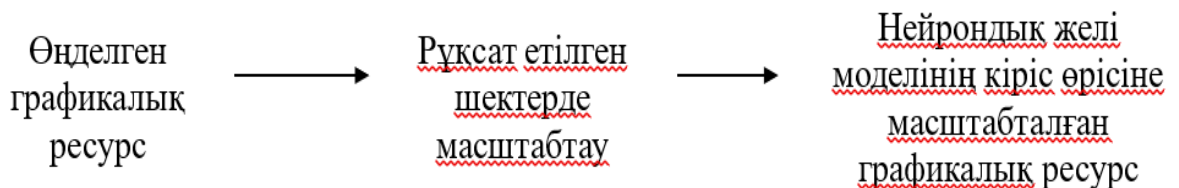
мұндағы $A(x, y) - x, y$; s_1, s_2 – кескіннің ені мен биіктігі координаттары бар нүктедегі пиксель түсінің қарқындылығы; * - конволюция операторы.

Жарықтық, контраст және типтік бұрмалануларды түзету процедурасы S индикаторының шамасы белгілі бір шекті мәннен аз болған жағдайда жүзеге асырылады.

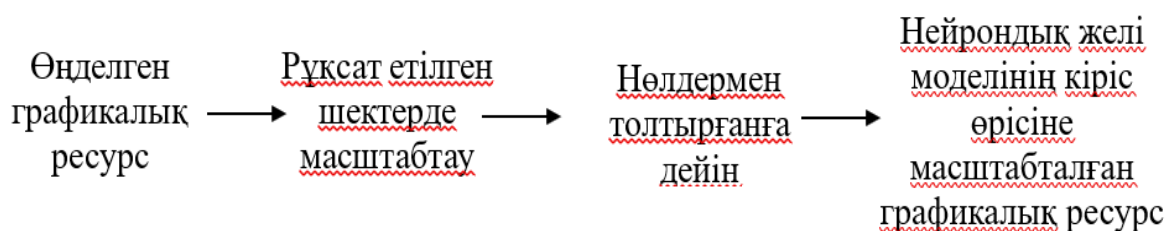
Негізгі нұсқаға [67, 68, 69] сәйкес көрсетілген шекті 150 - ге тең қабылдауға болады.

Графикалық ресурстың өлшемдерін тиімді масштабтау мүмкіндігін тексеру кезінде (2.1-2.6) өрнектері қолданылады. Екінші бөлімнің нәтижелеріне сәйкес $k_{max} = 2, k_{min} = 0,2, \vartheta = 1,3$.

Тиімді масштабтау мүмкін болған жағдайда немесе мүмкін болмаған жағдайда графикалық ресурстың өлшемдерін нейрондық желі моделінің кіріс өрісіне бейімдеу процедурасының схемасы сәйкесінше сурет 3.11 және 3.12 – де көрсетілген.

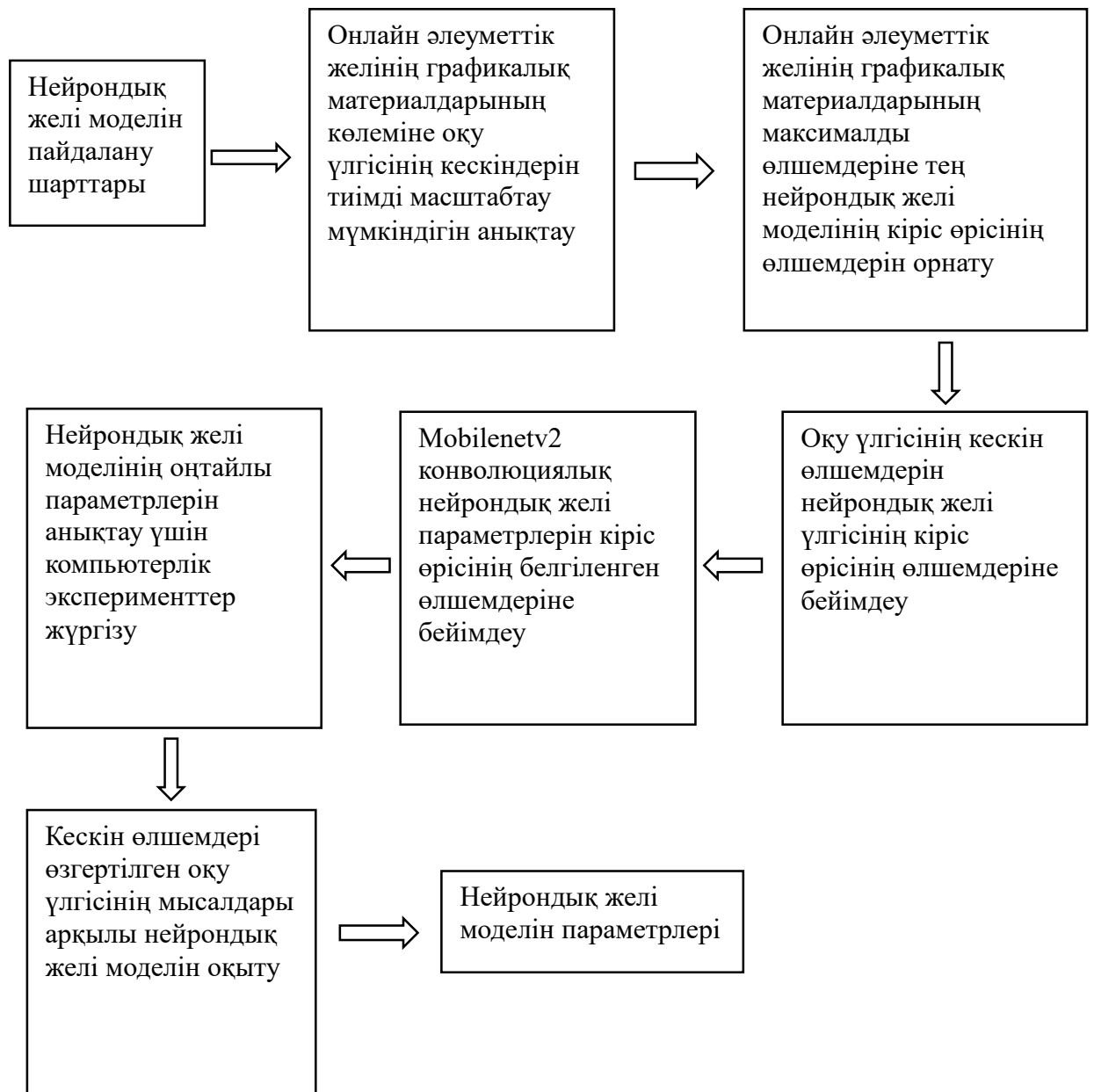


Сурет 3.11 – Тиімді масштабтау мүмкіндігі болған жағдайда графикалық ресурстың өлшемдерін бейімдеу процедурасының сұлбасы



Сурет 3.12 – Тиімді масштабтау мүмкін емес болған жағдайда графикалық ресурстың өлшемдерін бейімдеу процедурасының сұлбасы

Тиімді масштабтау мүмкіндігі болған жағдайда графикалық ресурстың өлшемдерін бейімдеу процедурасының иллюстрациясы сурет 3.13 – де және тиімді масштабтау мүмкін болмаған жағдайда графикалық ресурстың өлшемдерін бейімдеу процедурасы сурет 3.14 – тің көмегімен суреттелген.



Сурет 3.15 – Нейрондық желі моделін құру процедурасының сұлбасы

Онлайн әлеуметтік желінің графикалық материалдарының көлеміне оқу үлгісінің кескіндерін тиімді масштабтау мүмкіндігін анықтау кезеңі сурет 3.11 және 3.12 – де көрсетілген сұлбаларға сәйкес жүзеге асырылады.

Сондай-ақ, компьютерлік эксперименттер кезеңінде екінші бөлімнің нәтижелеріне сәйкес нейрондық желі моделінің келесі параметрлерін анықтау керек екенін атап өткен жөн:

- Конволюциялық қабаттар саны - K_C ;
- Конволюциялық қабаттардың әрқайсысындағы белгілер карталарының саны - $K_s(k_1), k_1 \in [1; K_C]$;
- Рекуррентті ұяшықтар типі - $T_{RNN} \in \{LSTM, GRU\}$;

- Рекуррентті қабаттар саны - K_{RNN} .
- Рекуррентті қабаттар ішіндегі рекуррентті ұяшықтар саны - $K_T(k_2), k_2 \in [1; K_{RNN}]$;
- CNN – модулі A_{CNN} нейрожелілік моделінде Attention механизмін қолдану орындылығы. Егер механизмді қолдану дұрыс болса, онда $A_{CNN} = 1$, басқа жағдайда $A_{CNN} = 0$;
- RNN – модулі A_{RNN} нейрожелілік моделінде Attention механизмін қолдану орындылығы. Егер механизмді қолдану дұрыс болса, онда $A_{RNN} = 1$, басқа жағдайда $A_{RNN} = 0$;
- CNN – модулі T_{ACNN} нейрожелілік моделінде Attention механизм типі;
- RNN – модулі T_{ARNN} нейрожелілік моделінде Attention механизм типі;
- K_D - толық байланысқан қабаттар саны;
- Әрбір толық байланысқан қабаттағы нейрондар саны - $K_N(k_3), k_3 \in [1; K_D]$

Нейрондық желі моделінің құрылымдық параметрлерінің оңтайлы мәндерін анықтауға арналған өрнек:

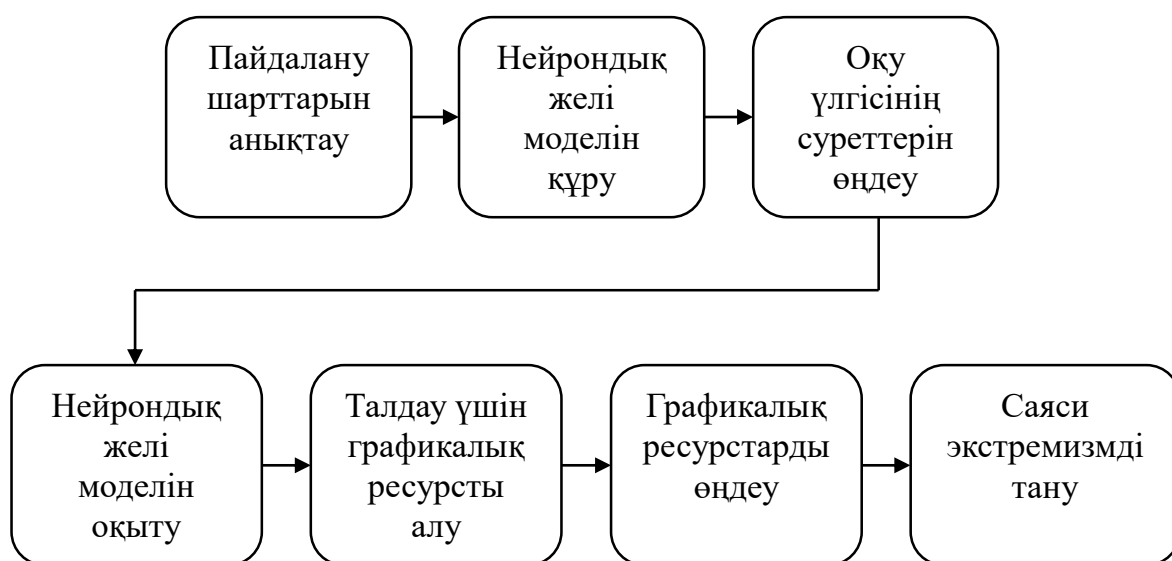
$$\left\{ \begin{array}{l} A_1 \left(K_C, K_S(k_1), T_{RNN}, K_{RNN}, K_T(k_2), A_{CNN}, A_{RNN}, T_{ACNN}, T_{ARNN}, K_D, K_N(k_3) \right) \rightarrow (4.12) \\ A_2 \leq A_2^{max} \end{array} \right.$$

мұндағы A_1 – тану дәлдігі; A_2 – нейрожелілік модельдің ресурс қарқындылығы; A_2^{max} – максималды рұқсат етілген ресурс қарқындылығы.

Айтып кететін жайт, Attention механизмінің түрі маңызды салмақ матрицасының қалыптасу механизмін анықтайды [70, 71]. Негізгі жағдайда Attention механизмінің екі түрін қолдануға болады: өзіндік зейін (self-attention) және көп фокустық зейін (MultiHead) [72, 73].

Онлайн әлеуметтік желілердің бейнелері мен бейнематериалдарында саяси экстремизмді анықтаудың әзірленген әдісін іске асыру сұлбасы 3.16 – суретте көрсетілген. Сұлба төмендегілерді ескере отырып жасалған:

- осы әдіс арқылы ақпаратты өңдеуді аналитикалық түрде сипаттайтын өрнектер (4.1-4.8),
- кескінді алдын-ала өңдеу қажеттілігін анықтау үшін негіз ретінде қолданылатын өрнектер (4.9-4.11),
- нейрондық желі моделінің құрылымдық параметрлерінің оңтайлы мәндерін анықтауда қолданылатын өрнектер (4.12),
- сызбалары 3.11 – 3.12 – суреттерде, 3.15 – суретте көрсетілген саяси экстремизмді анықтау, графикалық ресурстың өлшемдерін бейімдеу, нейрондық желі моделін құру бойынша әзірленген процедуралар.



Сурет 3.16 – Онлайн әлеуметтік желілердегі бейнелер мен бейнематериалдардағы саяси экстремизмді анықтау әдісі іске асыру сұлбасы

Сурет 3.16 – де көрсетілгендей әдісті жүзеге асыру 7 кезенді қамтиды.

1 кезең. Пайдалану шарттарын анықтау.

Кезеңнің орындалуы эксперименттік онлайн әлеуметтік желіні және қалыптастыру үшін тану жүйесін құруға бөлінген ресурстарды сараптамалық және аспаптық бағалаудан тұрады: талданатын онлайн әлеуметтік желінің графикалық ресурстары параметрлерінің мәндерін қамтитын кортеж (G); қол жетімді нейрондық желі модельдерінің параметрлерінің мәндерін қамтитын кортеж (N); тану процесін сипаттайтын жағдайлар кортежі (Q); нейрондық желі моделінің оқу үлгісінің көптеген мысалдары (DS); нейрондық желі модельдерін құру үшін қолданылатын көптеген сараптамалық мәліметтер (Z); нейрондық желі модельдерінің тиімділігінің көптеген критерийлері (A); графикалық ресурстарды алдын-ала өңдеу моделінің параметрлерінің мәндерін қамтитын кортеж (M).

2 кезең. Нейрондық желі моделін құру

2-кезеңнің кірісіне 1-кезеңді орындау кезінде анықталған G , N , Q , DS , Z , A , беріледі. 1 – 5 кезеңдерге сәйкес онлайн әлеуметтік желілердің графикалық ресурстарын талдаудың нейрондық желілік моделі негізінде жүзеге асырылады, мұндай модельді құру процедурасы 3.15 – суретте көрсетілген.

2-кезеңнің шығысы көрсетілген онлайн әлеуметтік желіде (\bar{D}) саяси экстремизмді анықтау міндетінің шарттарына бейімделген нейрондық желі моделінің архитектуралық параметрлері болып табылады.

3 кезең. Оқу үлгісінің суреттерін өңдеу

3 – кезеңнің кірісі 1 - кезеңде анықталған енеді: DS , M , сондай-ақ нейрондық желі моделінің кіріс өрісінің өлшемі ($s_1 \times s_2$) және түс пішімі

($type_{color}$). Өңдеу оқу үлгісінің кескіндерінің түс форматы мен өлшемдерін нейрондық желі моделінің кіріс өрісіне бейімдеу мақсатында жүзеге асырылады. Түс форматын беру жалпыға қол жетімді кодектердің көмегімен жүзеге асырылады, ал өлшемдерді бейімдеу графикалық ресурстардың өлшемдерін бейімдеудің ұсынылған процедурасына сәйкес графикалық ресурстарды алдын - ала өңдеудің ұсынылған моделі негізінде жүзеге асырылады, оның схемасы 3.11 – 3.12 – суретте көрсетілген. 3-кезеңнің шығысы – оқу үлгісінің көптеген өңделген мысалдары (\overline{DS}) болып табылады.

4 кезең. Нейрондық желі моделін оқыту.

4 – кезеңнің кірісіне мыналар енеді: 2 - кезеңде анықталған \overline{DS} ; 3 – кезеңде анықталған \overline{D} , сондай – ақ ($r_{lr} \in Q$) бөлінген ресурстар және 1 – кезеңде анықталған нейрондық желі моделінің рұқсат етілген ($t_{lr} \in Q$) оқу уақыты. Нейрондық желі моделін құру процедурасының (3.15 – сурет) 6 – шы кезеңінің нәтижелеріне сүйене отырып [74, 75], оқыту процесі $mini - batch$ механизмін қолдана отырып, қатені кері тарату алгоритмі арқылы жүзеге асырылады. 4 – кезеңнің шығысы, пайдаланылған нейрондық желі моделінің (D) параметрлерінің мәндері бар кортеж.

5 кезең. Талдау үшін графикалық ресурсты алу

5 – кезеңнің кірісіне мыналар беріледі: 1 кезеңде анықталған – G , сондай - ақ параметрлері нейрондық талдауға жататын O_{GM} – нысаны. Аталған объектіні алу көзі талданатын онлайн әлеуметтік желі болып табылады деп болжанады. Аталған объектіні әлеуметтік желіден алу үшін, сондай-ақ G негізінде талдауға жататын параметрлердің мәндерін анықтау үшін белгілі талдағыштарды қолдануға болады. 5 – кезеңнің шығысы онлайн әлеуметтік желінің талданатын графикалық ресурсының параметрлерінің мәндерін қамтитын GM – кортеж болып табылады.

6 кезең. Графикалық ресурстарды өңдеу

6 – кезеңнің кірісіне мыналар кіреді: 1, 4, 5 кезеңдерді орындау нәтижесінде алынған M , D , GM . Өңдеу сызбасы 4.1 – суретте көрсетілген саяси экстремизмді анықтау процедурасының 1 – 3 кезеңіне сәйкес онлайн әлеуметтік желілердің графикалық ресурстарын өңдеудің дамыған моделі негізінде жүзеге асырылады. 6 – кезеңнің шығысы \overline{GM} – нейрондық желіні талдауға жататын өңделген графикалық ресурстың параметрлерінің кортежі.

7 кезең. Саяси экстремизмді тану

7 – кезеңнің кірісіне мыналар кіреді: 4 және 6 кезеңдерде анықталған D және \overline{GM} . Саяси экстремизмді анықтаудың әзірленген процедурасына сәйкес (3.10-сурет) кезеңді іске асыру онлайн әлеуметтік желілердің графикалық ресурстарын талдаудың әзірленген нейрондық желілік моделінің шығыс сигналын анықтаудан тұрады. 7 – кезеңнің шығысы онлайн әлеуметтік желінің талданған графикалық ресурсында - Y_{GM} саяси экстремизмнің болуын көрсететін нейрондық желі моделінің шығыс сигналдарын қамтитын жиынтықтар болып табылады.

7 – кезеңнің шығысы – әдістің шығысы.

Жалпы ұсынылған әдіс арқылы алынған онлайн әлеуметтік желілердің графикалық материалдарындағы саяси экстремизмді анықтау нәтижелері, түр өрнектерін қолдана отырып онлайн әлеуметтік медиа ресурстарында саяси экстремизмнің болуын интегралды бағалауда ескерілуі мүмкін:

$$Y_{\Sigma} = k_T Y_T + k_{GM} Y_{GM}, \quad (4.13)$$

$$k_T(i) + k_{GM}(i) = 1, \quad i = 1 \dots N, \quad (4.14)$$

мұндағы Y_{Σ} – саяси экстремизмнің болуы/болмауы туралы интегралды бағалауды қамтитын жиын; Y_T, Y_{GM} – мәтіндік және графикалық ресурстарда саяси экстремизмнің бар/жоқтығын бағалайтын жиын; k_T, k_{GM} – салмақ коэффициенттерінің мәндері бар жиындар, N – салмақ коэффициенттері жиынының элементтерінің саны.

Зерттеудің алға қойған міндеті тек саяси экстремизмді анықтауды көздейтіндіктен, негізгі жағдайда саяси экстремизмнің болуын бағалауды оның болмауын өрнек арқылы бағалаумен байланыстыруға болады:

$$Y_1 = 1 - Y_2, \quad (4.15)$$

мұндағы Y_1, Y_2 – саяси экстремизмнің болуын, болмауын бағалау.

Көрсетілген болжам бағалаудың скалярлық мәндерін (4.13, 4.14) өрнектерде қолдануға мүмкіндік береді:

$$Y_{\Sigma} = k_T Y_T + k_{GM} Y_{GM}, \quad (4.16)$$

$$k_T + k_{GM} = 1, \quad (4.17)$$

мұндағы Y_{Σ}, Y_T, Y_{GM} – саяси экстремизмнің болуын бағалау, интегралды, мәтінде, графикалық материалдарда.

Нәтижелерді қолдана отырып, толық емес деректер жиынтығында оқытылған, құрастырылған нейрондық желі моделін пайдаланған кезде салмақ коэффициенттерінің мәндерін $k_T = 0,7$, $k_{GM} = 0,3$ деп қабылдауға болатындығы анықталды. Көрсетілген мәндерді (4.16) енгізіп, келесі нәтиже аламыз:

$$Y_{\Sigma} = 0,7Y_T + 0,3Y_{GM}, \quad (4.18)$$

Бастапқы жағдайда бұл өрнек онлайн әлеуметтік желі ресурстарында саяси экстремизмнің табылуын интегралды бағалауды есептеу үшін пайдаланылуы мүмкін.

Осылайша, жүргізілген зерттеулер нәтижесінде алғаш рет онлайн әлеуметтік желілердің бейнелері мен бейнематериалдарындағы саяси экстремизмді анықтау әдісі әзірлендігі ол ұсынылған алдын ала өңдеу және нейрондық желіні талдау модельдерін қолдану арқылы, сондай – ақ нейрондық желі моделінің кіріс өрісін графикалық ресурстар өлшемдерінің өзгергіштігіне бейімдеуге ұсынылған тәсіл арқылы онлайн әлеуметтік желілердің суреттері мен бейнематериалдарындағы саяси экстремизмді анықтау тиімділігін арттыруды қамтамасыз етеді. Бұл әдісті іске асыру нәтижелерін онлайн әлеуметтік медиа ресурстарында саяси экстремизмді тануды интегралды бағалауда пайдалану үшін математикалық аппарат ұсынылды. Сондай-ақ, онлайн әлеуметтік желілердің бейнелері мен бейнематериалдарында саяси экстремизмді анықтаудың ұсынылған әдісін жетілдіру бағытындағы зерттеудің одан әрі

жолдарын танудың нейрондық желілік модельдерін жетілдірумен, тиісті мазмұндағы графикалық материалдары бар репрезентативті мәліметтер базасын қалыптастырумен, сондай-ақ онлайн әлеуметтік желілердің мәтіндік және графикалық ресурстарын интеграцияланған талдау есебінен саяси экстремизмді анықтаудың тиімді тетігін әзірлеумен салыстырған жөн.

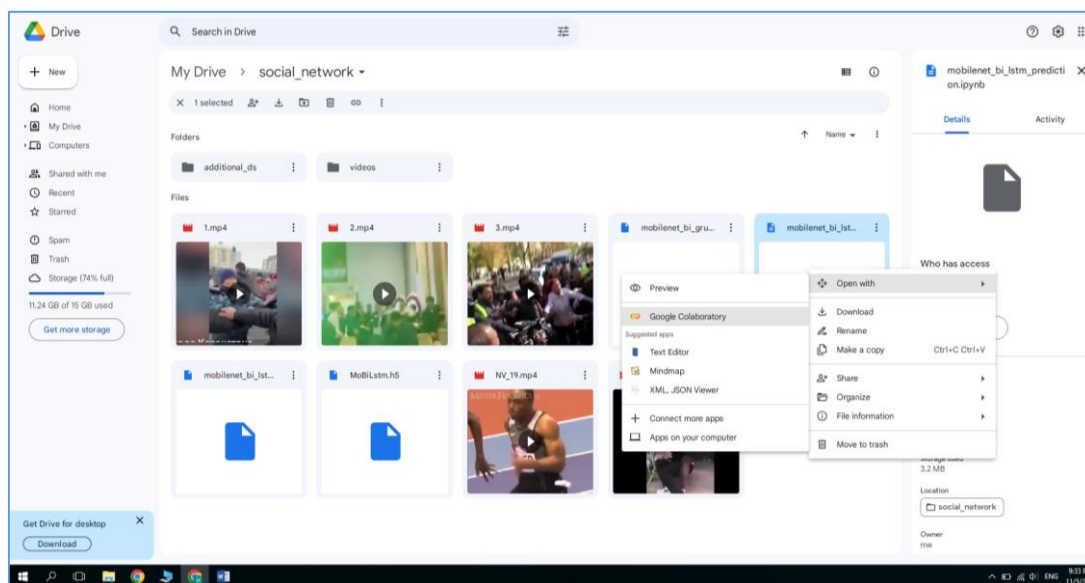
3.4. Онлайн әлеуметтік желілеріндегі саяси экстремизмді анықтау әдісін эксперименттік тексеру

Сәйкесінше [76, 77, 78], осы бөлімде ұсынылған эксперименттік зерттеулердің негізгі мақсаты онлайн әлеуметтік желілерінің суреттері мен бейнематериалдарында саяси экстремизмді анықтау әдісін - графикалық ресурстарды алдын ала өңдеу моделін графикалық ресурстарды талдаудың нейрондық желілік моделін құруда қолданылатын шешімдерді әзірлеуге қатысты диссертациялық зерттеу нәтижелерін растау болды.

Нәтижесінде эксперименттер келесі гипотезаларды эксперименттік тексеруге бағытталды:

Гипотеза 1. Саяси экстремизмді анықтаудың ұсынылған әдісін іске асыруда графикалық ресурстарды өңдеудің дамыған моделін қолдану онлайн әлеуметтік желілердегі суреттер мен бейнематериалдардағы саяси экстремизмді анықтаудың дәлдігін арттыруға мүмкіндік береді.

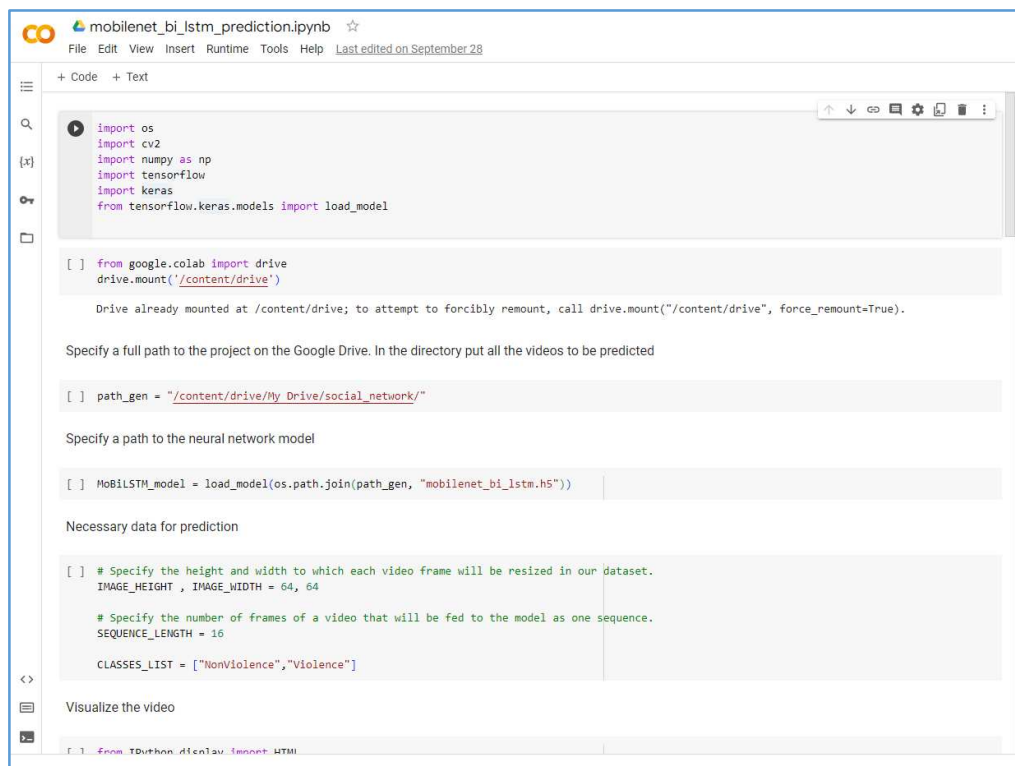
Гипотеза 2. Саяси экстремизмді анықтаудың ұсынылған әдісін іске асыру кезінде зерттелетін онлайн әлеуметтік желінің графикалық ресурстарын талдау жағдайларына бейімдеп, әзірленген нейрондық желі моделін пайдалану суреттер мен бейнематериалдардағы саяси экстремизмді анықтаудың тиімділігін арттыруға мүмкіндік береді.



Сурет 3.17 – Google Colab ортасын баптау

Зерттеудің мақсаты мен гипотезаларына сүйене отырып, эксперименттік бағдарламалық – аппараттық кешен әзірленді:

- ұсынылған модельге сәйкес (2.1-2.24) онлайн әлеуметтік желілердің графикалық ресурстарын алдын ала өңдеуді жүзеге асыру;
- әзірленген нейрондық желі моделін қолдану қажет болған жағдайда құрылымдық параметрлерді өзгерте отырып, графикалық ресурстарды талдауды жүзеге асыру.



```
import os
import cv2
import numpy as np
import tensorflow
import keras
from tensorflow.keras.models import load_model

[ ] from google.colab import drive
drive.mount('/content/drive')

Drive already mounted at /content/drive; to attempt to forcibly remount, call drive.mount("/content/drive", force_remount=True).

Specify a full path to the project on the Google Drive. In the directory put all the videos to be predicted

[ ] path_gen = "/content/drive/My Drive/social_network/"

Specify a path to the neural network model

[ ] MoBiLSTM_model = load_model(os.path.join(path_gen, "mobilenet_bi_lstm.h5"))

Necessary data for prediction

[ ] # Specify the height and width to which each video frame will be resized in our dataset.
IMAGE_HEIGHT, IMAGE_WIDTH = 64, 64

# Specify the number of frames of a video that will be fed to the model as one sequence.
SEQUENCE_LENGTH = 16

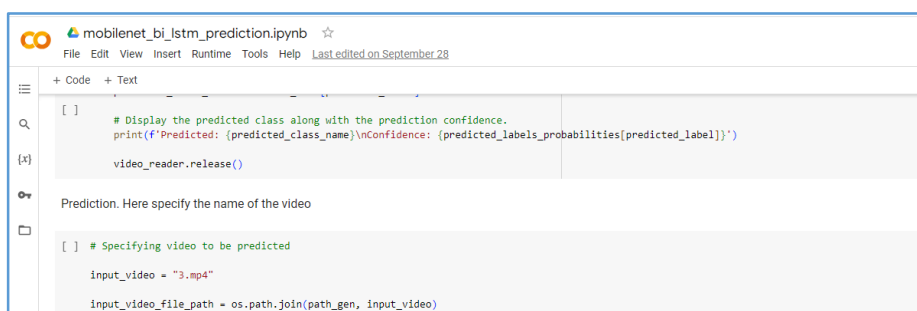
CLASSES_LIST = ["NonViolence", "Violence"]

Visualize the video

[ ] from IPython.display import HTML
```

Сурет 3.18 – Жоба оналасқан бума жолын және нейрондық желі моделінің атауын көрсету

Графикалық ресурстарды алдын-ала өңдеуге байланысты эксперименттер жүргізу үшін MATLAB бағдарламалық жасақтама кешені қолданылды, бұл оның сенімділігімен, сынақтан өтуімен және қажетті функционалдылықтың болуымен түсіндіріледі.



```
[ ] # Display the predicted class along with the prediction confidence.
print(f'Predicted: {predicted_class_name}\nConfidence: {predicted_labels_probabilities[predicted_label]}')

video_reader.release()

Prediction. Here specify the name of the video

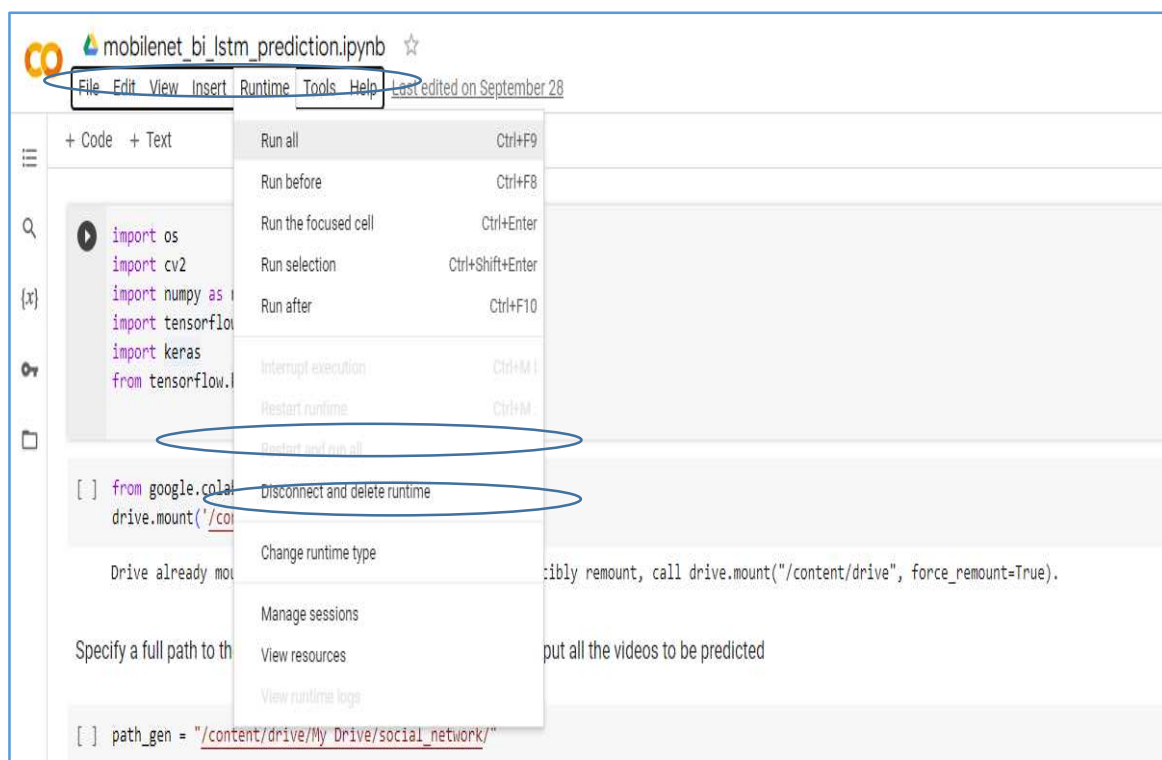
[ ] # Specifying video to be predicted

input_video = "3.mp4"

input_video_file_path = os.path.join(path_gen, input_video)
```

Сурет 3.19 – Талданатын графикалық материалы бар файл атауын көрсету

Нивелирлеу үшін кескінді өңдеу мысалы бұлыңғыр, көшедегі бейне түсірілімге тән сурет көрсетілген. Графикалық ресурстарды өңдеуге қатысты эксперименттерде дербес компьютер (AMD Ryzen 5 5600X (3.7 - 4.6 ГГц) / RAM 16 ГБ / SSD 1 ТБ / nVidia GeForce RTX 3060 Ti, 8 ГБ) пайдаланылды.



Сурет 3.20 – Бағдарламаны анықтау режимінде іске қосылуы

Графикалық ресурстарды нейрондық желіні талдауға байланысты эксперименттер жүргізу үшін түпнұсқа бағдарламалық қамтамасыз ету әзірленді. Бағдарламалық қамтамасыз ету TensorFlow кітапханасының көмегімен Python бағдарламалау тілінде жазылған. Бағдарламалық жасақтаманың жұмысы Google Colab ортасына бағытталған, бұл бұлтты есептеулерге еркін қол жеткізу мүмкіндігімен түсіндіріледі. Пайдаланушы интерфейсін әзірлеу Google Colab ортасында оны орналастыру ерекшеліктерін ескере отырып, анықтау жүйесін эргономикалық пайдалануды қамтамасыз ету тұрғысынан жүзеге асырылды. Бағдарламалық құрал файлдары «social_network» бумасына орналастырылуы керек екенін ескереміз.

Бағдарлама Mobilenet_Bi_Lstm_Prediction файлы арқылы анықтау режимінде іске қосылады. іrunb Google Colab ортасында орналастырылған. Іске қосу процедурасы 3.17-3.20 суреттерде көрсетілген.

Нейрондық желіні талдау нәтижесінің иллюстрациясы сурет 3.21 – те көрсетілген.

```
mobilenet_bi_lstm_prediction.ipynb
File Edit View Insert Runtime Tools Help Last edited on September 28

+ Code + Text

[ ] # Display the predicted class along with the prediction confidence.
print(f'Predicted: {predicted_class_name}\nConfidence: {predicted_labels_probabilities[predicted_label]}')

video_reader.release()

Prediction. Here specify the name of the video

[ ] # Specifying video to be predicted

input_video = "3.mp4"

input_video_file_path = os.path.join(path_gen, input_video)

# Perform Single Prediction on the Test Video.
predict_video(input_video_file_path, SEQUENCE_LENGTH)

1/1 [-----] - 3s 3s/step
Predicted: Violence
Confidence: 0.9974697828292847

# Play the video
Play_Video(input_video_file_path)
```

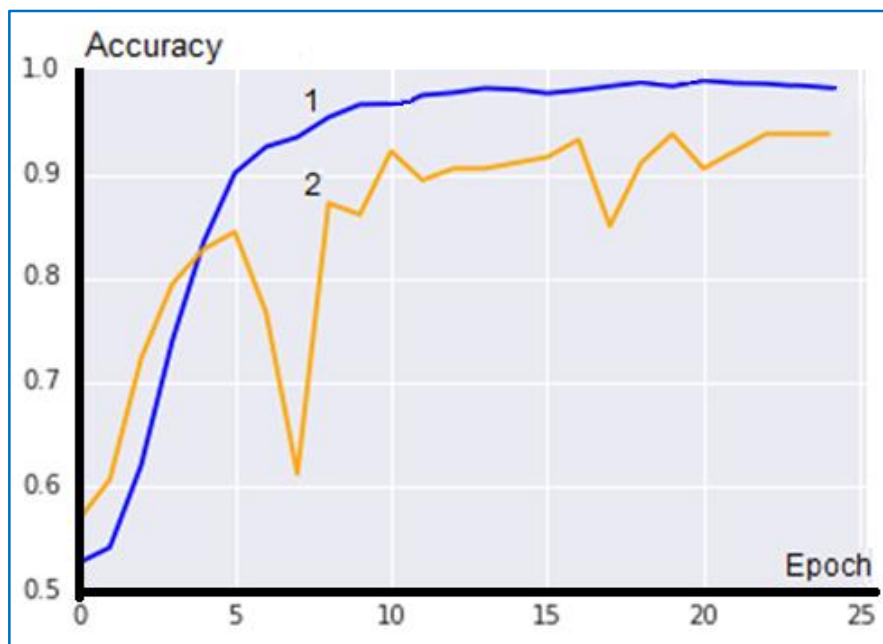
The screenshot shows a Jupyter Notebook interface. The top part contains code for displaying prediction results and releasing a video reader. Below that is a prompt for video prediction. The next code block specifies the video file path and performs a prediction. The output shows the predicted class as 'Violence' with a confidence of approximately 0.997. At the bottom, there is a code cell to play the video, which is followed by a video player showing a crowd of people.

Сурет 3.21 – Нейрондық талдау нәтижелерін көрсету

Ұсынылған алдын ала өңдеу моделін (2.1-2.24) пайдалану арқылы онлайн әлеуметтік желілерінің графикалық материалдарын талдаудың нейрондық желілік құралдарының дәлдігін арттыру мүмкіндігіне қатысты 1 гипотезаны растау үшін компьютерлік эксперименттер жүргізілді. Эксперименттер барысында әзірленген нейрондық желі моделінің негізгі нұсқасы қолданылды.

Желі Real Life Violence Situations Dataset [79] жалпыға қолжетімді дерекқорынан оқу мысалдарымен оқытылды. Дерекқорда әртүрлі орталар мен жағдайларда YouTube бейнелерінен жиналған 1000 зорлық-зомбылық мазмұнды бейнелері және 1000 зорлық-зомбылық мазмұны жоқ бейнелерден құралған. Іріктеме 9:1 қатынасында оқу және валидация болып бөлінеді. Оқу (1) және валидациялық (2) деректерді тану дәлдігінің графиктері сурет 3.22 – да көрсетілген. Суретте 3.6 – да көрсетілгендей оқытудың 25 дәуірінен кейін оқу деректерін тану дәлдігі шамамен 0,97, ал валидациялық деректер шамамен 0,95 құрайды. Оқытылған желіні тексеру үшін валидация үлгісінен ең төменгі 10 мысал таңдалды. Бұл мысалдарды танудың орташа дәлдігі шамамен 0,86 болды. Содан соң бұл мысалдар алдын-ала өңдеудің дамыған моделін қолдана отырып өңделді (2.1-2.24). Өңделген мысалдарды танудың орташа дәлдігі 0,94 болды.

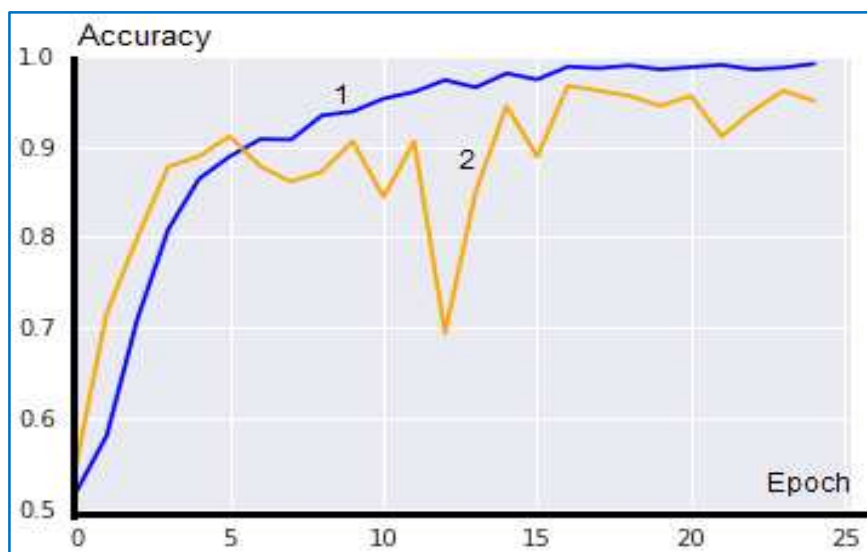
Осылайша, ұсынылған алдын-ала өңдеу моделін қолдану графикалық материалдарды алдын-ала өңдеу арқылы нейрондық желілік талдаудың тиімділігін арттыру саласында бейнематериалдарды тану дәлдігін шамамен 1,09 есе арттыруға мүмкіндік беріп, [80, 81, 82] жұмыс нәтижелеріне сәйкес келеді.



Сурет 3.22. – Оқу және валидация деректерін тану дәлдігінің графиктері

Демек, эксперимент нәтижелері 1-гипотезаның дұрыстығын растайды және сәйкесінше графикалық ресурстарды өңдеу үшін ұсынылған модельдің тиімділігін растайды.

Ұсынылған нейрондық желі моделінің тиімділігіне және тұтастай анықтау әдісіне қатысты 2-гипотезаны растау үшін компьютерлік эксперименттер жүргізілді, оларда (3.8) сәйкес әзірлеудің негізгі нұсқасы үшін анықтау дәлдігінің мәні анықталды. нейрондық желі моделі, (4.12) сәйкес оңтайландырылған нейрондық желі моделі, сондай-ақ (3.13) жиынынан конволюционды нейрондық желі негізінде құрастырылған конволюциялық модулі нейрондық желі модельдері.



Сурет 3.23 – Оңтайландырылған нейрондық желі моделі үшін оқу және валидация деректерін тану дәлдігінің графиктері

Тәжірибелер барысында 1024x1024 кіріс өрісі бар оңтайландырылған нейрондық желі моделінің негізгі нұсқасынан негізгі айырмашылығы LSTM қабаттарының әрқайсысындағы LSTM ұяшықтары санының 32-ден 128-ге дейін өзгеруі, сондай-ақ толық қосылған қабаттардың әрқайсысында нейрондар санының екі есе артуы. Нейрондық желі моделінің конволюционды модулінің параметрлері 2x2 конволюциялық ядросы бар мүмкіндік карталарының өлшемін сәйкес өзгертуге әкелетін 1024x1024 өлшемді кіріс кескінін өңдеу қажеттілігі негізінде анықталады. Сонымен, соңғы конволюциялық қабатта 32x32 мүмкіндік картасының өлшемі бар. Бұл эксперименттердің басты нәтижелері сурет 3.23 және кесте 3.5 – де көрсетілген.

Кесте 3.5 – Әр түрлі нейрондық модельдер үшін ресурстарды қажет ететін және дәлдік көрсеткіштері

| Базалық нейрожелілік модель | Ресурс сыйымдылығы (салмақ коэффициенттерінің жуық саны, $\times 10^6$) | Дәлдік |
|---|--|--------|
| VGG-16 | 138 | 0,92 |
| VGG-19 | 144 | 0,94 |
| GoogleNet | 5 | 0,94 |
| Inception-v3 | 23,8 | 0,98 |
| SqueezeNet | 1,2 | 0,89 |
| ResNet-50 | 25,6 | 0,98 |
| MobileNetV2 негізінде әзірленген модель | 2,2 | 0,97 |
| MobileNetV2 негізінде оңтайландырылған модель | 2,4 | 0,99 |

Сурет 3.23 – те көрсетілгендей, оқытудың 25 дәуірінен кейін MobileNetV2 негізіндегі оңтайландырылған модельдің тану дәлдігі шамамен 0,99, ал валидация деректері шамамен 0,97 құрайды. Сонымен қатар, кесте 3.5-те көрсетілгендей, оңтайландырылған параметрлері бар әзірленген нейрондық желі моделін тану дәлдігі басқа модельдерді тану дәлдігінен біршама асып түседі және ресурстардың сыйымдылығы жағынан олардың көпшілігінен айтарлықтай асып түседі. Осылайша, эксперименттердің нәтижелері 2-гипотезаның дұрыстығын, сәйкесінше диссертациялық шешімдердің тиімділігін растайды.

Онлайн әлеуметтік желілерінің графикалық ресурстарында саяси экстремизмді анықтау әдістемесін жетілдіру саласындағы одан әрі зерттеу жолдарын құрастырылған нейрондық желі моделіне Attention механизмін қосумен қатар саяси экстремизмді анықтауға арналған нейрондық желі моделін оқыту үшін репрезентативті оқыту үлгілерін қалыптастыру ұсынылады.

Үшінші бөлім бойынша қорытынды. Машиналық оқыту (ағылшынша machine learning, ML) – жасанды интеллект әдістерінің класы, оған тән белгі мәселені тікелей шешу емес, көптеген ұқсас мәселелердің шешімдерін қолдану арқылы оқыту болып табылады. Мұндай әдістерді құру үшін математикалық статистика, сандық әдістер, математикалық талдау, оңтайландыру әдістері, ықтималдықтар теориясы, графикалық теориялар, сандық түрдегі деректермен жұмыс істеудің әртүрлі әдістері қолданылады [83, 84, 85].

Мәліметтерді талдауға негізделген машиналық оқыту технологиясы 1950 жылы, дойбы ойынына арналған алғашқы бағдарламалар жасала бастаған кезден басталады. Компьютерлердің есептеу күшінің өсуіне байланысты олардың құратын заңдылықтары мен болжамдары бірнеше есе күрделене түсті және машиналық оқытудың көмегімен шешілетін мәселелер мен есептер ауқымы кеңейді.

Оқытудың келесідей түрі бар:

1) Прецеденттер бойынша оқыту немесе индуктивті оқыту деректердегі эмпирикалық заңдылықтарды анықтауға негізделген.

2) Дедуктивті оқыту сарапшылардың білімін формализациялауды және оларды білім базасы түрінде компьютерге беруді қамтиды.

Бақыланатын оқыту – бұл ең көп таралған жағдай. Әр жағдай «объект, жауап» жұбы болып табылады. Жауаптардың объектілердің сипаттамаларына функционалды тәуелділігін табу және объектінің сипаттамасын кіріс ретінде қабылдап, шығыста жауап қайтаратын алгоритм құру қажет болады. Сапа функционалы әдетте барлық үлгі объектілері үшін алгоритм құрған жауаптардың орташа қателігі ретінде анықталады.

– Жіктеу есебі мүмкін болатын жауаптар жиынтығының ақырлы болуымен ерекшеленеді. Оларды класс белгілері деп атайды. Класс – бұл белгі мәліметі бар барлық объектілер жиынтығы.

– Регрессия есебі жауаптың нақты сан немесе сандық вектор болуымен ерекшеленеді.

– Дәреже тағайындау (learning to rank) есебі жауаптардың бірден объектілер жиынтығында алынып, содан кейін жауаптардың мәндері бойынша сұрыпталуымен ерекшеленеді. Жіктеу немесе регрессия есептеріне дейін қысқартылуы мүмкін. Ол көбінесе ақпаратты іздеуде және мәтінді талдауда қолданылады.

– Болжау есебі (forecasting) объектілердің болашаққа болжам жасау қажет болған уақыт қатарының сегменттері болуымен ерекшеленеді. Болжау есебін шешу үшін регрессияны немесе жіктеу әдістерін бейімдеуге болады.

Бақыланбайтын оқыту. Бұл жағдайда жауаптар берілмейді және объектілер арасындағы тәуелділікті іздеу керек болады.

– Кластерлеу есебі объектілердің жұптық ұқсастығы туралы деректерді қолдану арқылы оларды кластерге топтастыруды қарастырады. Сапа функционалын әр түрлі әдіспен, мысалы, орташа кластераралық және кластерішілік арақашықтықтардың қатынасы ретінде анықтауға болады.

- Қауымдастық ережелерін іздеу есебі (association rules learning). Бастапқы мәліметтер сипаттамалар түрінде ұсынылады.

Бекіту арқылы оқыту. Нысан ретінде «жағдай, қабылданған шешім» жұптары қарастырылады, жауаптар - қабылданған шешімдердің дұрыстығын сипаттайтын функционалдық сапа мәндері (қоршаған ортаның реакциясы). болжау есебіндегідей, мұнда да уақыт факторы маңызды рөл атқарады. Қолданбалы есептердің мысалдары: инвестициялық стратегияларды қалыптастыру, технологиялық процестерді автоматты басқару, роботтарды өздігінен оқыту және т.б. [86]

Оқыту барысында пайдаланылатын мәліметтер жинағы $A = \{A_1, A_2, \dots, A_{|A|}\}$ атрибуттар жиынтығы арқылы сипатталады, мұндағы $|A|$ атрибуттар санын немесе A жинағының өлшемін білдіреді. Сонымен қатар, мәліметтер жинағында класс атрибуты деп аталатын арнайы мақсатты C атрибуты болады. C класс атрибуты дискретті мәндер жинағына ие, яғни $\{c_1, c_2, \dots, c_{|C|}\}$, мұндағы $|C|$ - класстар саны және $|C| \geq 2$. Класс мәні класс белгісі деп те аталады.

Кесте 3.6 – Машиналық оқыту әдістері көмегімен мәтінді экстремистік және бейтарап санаттарға жіктеу нәтижесі

| Machine learning algorithm | Accuracy | F1-Score | AUC-ROC |
|-------------------------------------|----------|----------|---------|
| Logistic regression | 0.92 | 0.93 | 0.92 |
| k-nearest neighbors | 0.76 | 0.78 | 0.75 |
| Decision Tree | 0.82 | 0.85 | 0.80 |
| Random Forest | 0.90 | 0.91 | 0.90 |
| Gradient Boosting | 0.88 | 0.90 | 0.87 |
| SVM | 0.58 | 0.66 | 0.56 |
| Naïve Bayes | 0.84 | 0.84 | 0.85 |
| LSTM_POLIT (предлагаемая модель) | 0.94 | 0.95 | 0.93 |

Оқытуға арналған мәліметтер жинағы – реляциялық кесте. Әрбір мәліметтер жазбасы машиналық оқыту тілінде мысал, экземпляр, оқиға немесе вектор деп аталады.

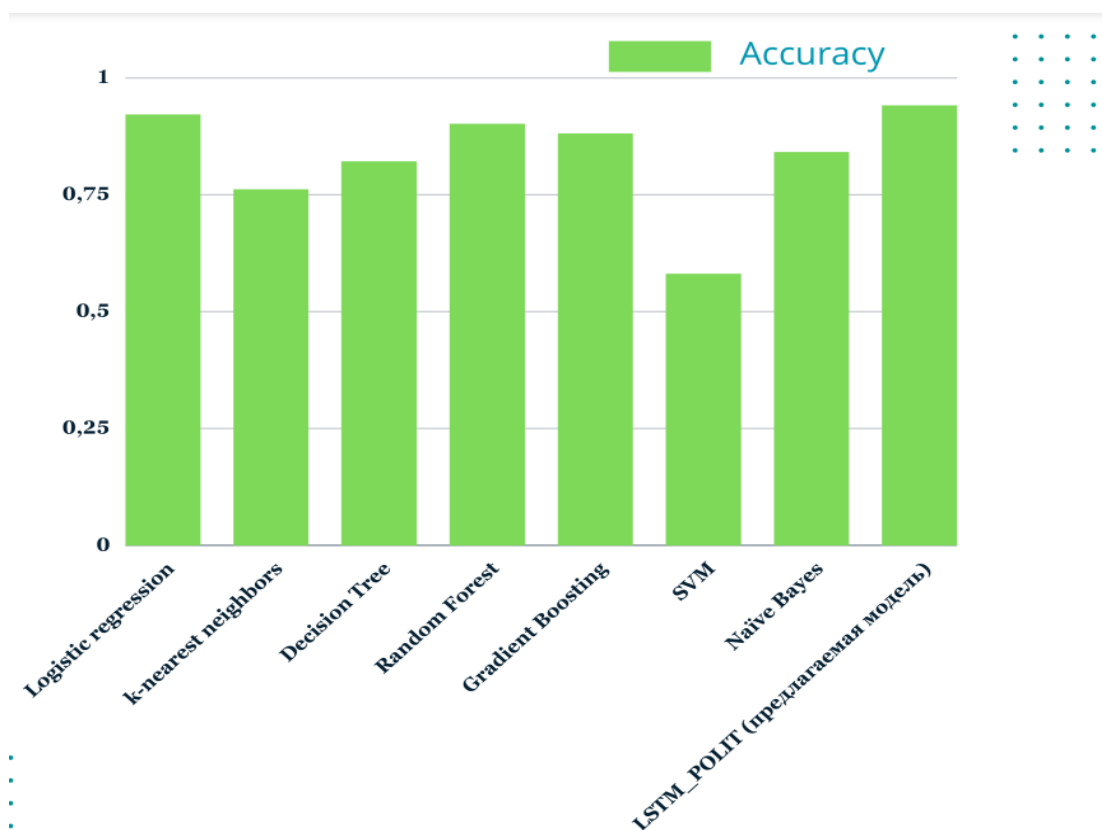
Мәліметтер жинағы негізінен мысалдардан тұрады. Оқыту мақсаты – D мәліметтер жинағын ескере отырып, A -дағы атрибуттар мен C -дағы класстардың мәндерін сәйкестендіруге арналған жіктеу/болжау функциясын құру болып табылады. Аталған функция болашақта кездесетін жаңа мәліметтердің

класстарының мәндерін болжау үшін пайдаланылады. Бұл функция жіктеу моделі немесе классификатор деп аталуы да мүмкін.

Оқыту үшін қолданылатын мәліметтер жиынтығы оқыту деректері (немесе оқыту жиынтығы) деп аталады. Модель оқыту алгоритмі арқылы оқыту деректері негізінде зерттелгеннен немесе құрастырылғаннан кейін, модельдің дәлдігін бағалау үшін тестілік мәліметтер жиынтығымен (немесе көрінбейтін мәліметтермен) бағаланады. Тест деректері жіктеу моделін зерттеуде пайдаланылмайды.

Тестілік деректердегі мысалдарда әдетте класс белгілері болады. Оқыту және тестілеу үшін қол жетімді мәліметтер (класстары бар) әдетте екі қиылыспайтын ішкі жиындарға бөлінеді: оқыту жиынтығы (оқыту үшін) және тест жиынтығы (тестілеу үшін) [87, 88, 89].

Диссертациялық жұмыстың мақсатына сай дәстүрлі машиналық оқыту әдістерін қолдану арқылы эксперименттер жүргізілді. Веб-ресурстардағы экстремистік мәтіндерді анықтау үшін шешім ағашы, мультиномиялық аңқау Байес, кездейсоқ орман, сызықтық регрессия және тірек векторлар машинасы сияқты дәстүрлі әдістер қолданылып, олардың жіктеу нәтижелері салыстырылды.



Сурет 3.24 – Ұсынылған әдісті басқа алгоритмдермен салыстыру нәтижесі

Өңделген графикалық ресурстардағы саяси экстремизмді тануға арналған нейрондық желілер ішінен бірнеше түріне эксперименттік зерттеулер жүргізілген болатын.

Қорытындылай келе, ұсынылатын модель машиналық оқыту әдістерімен салыстырғанда барлық бағалау параметрлері бойынша жоғары екендігін байқаймыз және нәтижесінде ұсынылатын модель онлайн әлеуметтік желілердегі қазақ тіліндегі саяси экстремистік мәтіндерді және графикалық ресурстарды жоғары дәлдікпен анықтай алады деген қорытындыға келеміз.

ҚОРЫТЫНДЫ

Әлеуметтік медиа платформалары адамдардың көзқарастарына, пікірлеріне және түсініктеріне әсер ету арқылы экстремизмнің таралуына ықпал етуде басты рөл атқарады. Бұл платформаларды экстремистік үгіт-насихат тарату, жастарды радикалдандыру және өз қатарына тарту үшін көбірек пайдалануда. Сондықтан әлеуметтік желілердегі экстремизмді анықтау бойынша зерттеулер оның әсері мен зиянды әсерін тежеу үшін қажет. Экстремизмді анықтау бойынша бар әдебиеттерге шолу оның нақты идеологиямен, экстремизмді мәтіндік түсінігі шектеулі екілік классификациямен және деректер сапасын тексеру үшін деректерді қолмен шолу әдістерімен шектелетінін көрсетеді. Қолданыстағы зерттеулерде зерттеушілер бір идеологиямен шектелген деректер жиынын пайдаланды.

Бұл диссертациялық жұмыста онлайн әлеуметтік желілердің мәтіндік және графикалық ресурстарында саяси экстремизмді анықтау әдістері мен моделін құру бойынша жұмыс жүргізіліп, келесі нәтижелерге қол жеткізілді:

- 1 Алғаш рет онлайн әлеуметтік желілерде саяси экстремизм белгілерін анықтайтын қазақ тіліндегі саяси экстремизм мәтіндер корпусы құрылды;
- 2 Алғаш рет қазақ тілінің ерекшеліктерін ескере отырып, белгілер жиынтығын қалыптастыру әдісі әзірленді және онлайн әлеуметтік желілерде қазақ тіліндегі саяси экстремизм мәтіндерін анықтау моделі құрылды;
- 3 Саяси экстремизмді анықтау үшін онлайн әлеуметтік желілердің графикалық ресурстарын өңдеу және нейрожелілік талдау моделі әзірленді;
- 4 Онлайн әлеуметтік желілердің графикалық ресурстарында саяси экстремизмді анықтаудың нейрондық әдісі жасалды;
- 5 Құрастырылған модельдер мен әдістердің нәтижесінде онлайн әлеуметтік желілердегі қазақ тіліндегі экстремистік мәтіндерді және графикалық ресурстарды анықтауға арналған бағдарламалық жабдықтама құрылды.

Бұл зерттеудің жаңалығы қазақ тіліндегі экстремистік мәтіндерді анықтау үшін терең нейрондық желі моделін жасау болып табылады. Алдын ала стемминг алгоритмі орындалған биграммдарға TF-IDF әдісін қолдану негізінде терең нейрондық желі моделі құрастырылды және нәтижелер қазақ тіліндегі экстремистік бағыттағы мәтіндерді анықтау міндеті үшін ең жоғары дәлдікпен классикалық машиналық оқыту әдістерімен салыстырғанда экстремистік мәтіндерді анықтауда ұсынылған модельдің тиімділігін көрсетеді. Сонымен қатар графикалық ресурстарды өңдеу нәтижесінде әлеуметтік желілеріндегі бейне және бейнематериалдардағы саяси экстремизмді анықтаудың нейрожелілік моделі әзірленді. Осылайша, экстремистік бағыттағы қазақ

тіліндегі мәтіндерді және графикалық ресурстардағы табу міндеті үшін терең нейрондық желі жоғары өнімділік беріп, өзінің тиімділігін көрсетті.

Диссертациялық жұмыстың теориялық маңыздылығы экстремистік іс-әрекеттер мен ұйымдарды анықтау әдістері мен алгоритмдері саласындағы білім жиынтығына негізделген. Алынған іргелі нәтижелерді әлемдік ғылыми қауымдастық пайдалана алады.

Ғылыми зерттеу нәтижелерін ақпараттық қауіпсіздікті, сыни инфрақұрылымды қамтамасыз ету, интернет-экстремизммен күрес жөніндегі уәкілетті органдар пайдалануы мүмкін.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

- 1 Sánchez-Rebollo C., Puente C., Palacios R., Piriz C., Fuentes J.P., Jarauta J. Detection of Jihadism in Social Networks Using Big Data Techniques Supported by Graphs and Fuzzy Clustering // Complexity. – 2019. – Vol.2019.
- 2 Gaikwad M., Ahirrao S., Phansalkar S., Kotecha K. Online Extremism Detection: A Systematic Literature Review with Emphasis on Datasets, Classification Techniques, Validation Methods, and Tools // IEEE Access. – 2021.
- 3 Экстремизмге қарсы іс-қимыл туралы. Қазақстан Республикасының 2005 жылғы 18 ақпандағы N 31 Заңы.
- 4 Қазақстан Республикасында діни экстремизм мен терроризмге қарсы іс-қимыл жөніндегі 2018 – 2022 жылдарға арналған мемлекеттік бағдарламаны бекіту туралы. Қазақстан Республикасы Үкіметінің 2018 жылғы 15 наурыздағы № 124 қаулысы. <https://adilet.zan.kz/kaz/docs/P1800000124>
- 5 ҚР тыйым салынған шетелдік ұйымдардың тізіміБаспаға шығару нұсқасы. Соңғы өзгеріс: 20.09.2022
- 6 Тоқаев «ақпараттық қауіпсіздік» орталығын құруды ұсынды. <https://qazaqtimes.com/article/63900>
- 7 Akram M., Nasar A., Rehman A., Misuse of charitable giving to finance violent extremism; A futuristic actions study amidst COVID-19 pandemic // Social Sciences & Humanities Open. – 2021. –Vol.4, №1. –P.1–7.
- 8 COVID-19 and Terrorism in the West: Has Radicalization Really Gone Viral? <https://www.justsecurity.org/75064/covid-19-and-terrorism-in-the-west-has-radicalization-really-gone-viral/detect>. 03.01.2022.
- 9 Hate in the time of coronavirus: exploring the impact of the COVID-19 pandemic on violent extremism and terrorism in the West <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7790481/>. 06.04.2022.
- 10 https://online.zakon.kz/Document/?doc_id=30004865
- 11 Чернышёв Е. Касперская: Окно в преступный мир у каждого ребенка в кармане // НАКАНУНЕ.РУ : [сайт]. URL: <https://www.nakanune.ru/news/2021/05/12/22601520/> (дата обращения: 12.11.2021).
- 12 Гайквад М., Ахиррао С., Фансалкар С., Котеча К. Обнаружение экстремизма в Интернете: систематический обзор литературы с упором на наборы данных, методы классификации, методы проверки и инструменты. *Доступ IEEE*. 2021 год; **9** : 48364–48404. дои: 10.1109/ACCESS.2021.3068313. [[CrossRef](#)] [[Академия Google](#)]
- 13 Ш.Ж. Мусиралиева, М.А. Болатбек, М. Сағынай, Ж.Ы. Елтай, К.Б. Багитова. Экстремистік мәліметтер түсінігі және экстремизмге қарсы күрес жобаларына жүйелік шолу. NEWS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN PHYSICO-MATHEMATICAL SERIES ISSN 1991-346X Volume 3. Number 347 (2023). 112–130. <https://journals.nauka-nanrk.kz/physics-mathematics/article/view/5792/4039>

14 Кеннеди Б. Корпус ненависти: сборник из 27 тысяч постов, аннотированных на разжигание ненависти. 2020. <https://psyarxiv.com/hqjxn/>

15 Аббар М.Ф., Арефин М.С., Хоссейн М.С. Структура анализа твитов в реальном времени для выявления террористической деятельности. Материалы 2-й Международной конференции по электротехнике, компьютерной и коммуникационной технике, ECCE 2019; Халдия, Индия; Март 2019 г. стр. 1–6. [[CrossRef](#)] [[Академия Google](#)]

16 Асиф М., Иштиак А., Ахмад Х., Альджуайд Х., Шах Дж. Анализ настроений экстремизма в социальных сетях на основе текстовой информации. *Телематика и информатика*. 2020; **48** дои: 10.1016/j.tele.2020.101345. 101345 [[CrossRef](#)] [[Академия Google](#)]

17 Яки С., Де Смедт Т. Правые немецкие высказывания ненависти в Твиттере: анализ и автоматическое обнаружение. 2019. <https://arxiv.org/abs/1910.07518#:~:text=Right%2Dwing%20Немецкий%20Hate%20Speech%20on%20Twitter%3A%20Анализ%20and%20Automatic%20Detection,-Sylvia%20Jaki%2C%20Tom%26text=Обсуждение%20о%20социальной%20сети, как от%20to%20общаются%20с%20ит> .

18 Бергер Дж. М. Перепись альтернативных правых в Твиттере: определение и описание аудитории альтернативного правого контента в Твиттере. 2018. <https://www.voxpol.eu/new-research-report-the-alt-right-twitter-census-by-jm-berger/>

19 Фернандес М., Асиф М., Алани Х. Понимание корней радикализации в Твиттере. Материалы 10-й конференции АСМ по веб-науке; май 2018 г.; Бостон, Массачусетс, США. стр. 1–10. [[CrossRef](#)] [[Академия Google](#)]

20 Багитова К.Б., Мусиралиева Ш.Ж, Болатбек М.А, Оспанов Р.К. Разработка программного обеспечения ExWeb для выявления экстремистского контента в сети Интернет. УДК 004.056.5. «Известия НАН РК. Серия физика и информатики». ISSN 2518-1726 (Online), ISSN 1991-346X (Print). SERIES PHYSICS AND INFORMATION TECHNOLOGY 2 (346) APRIL – JUNE 2023. Стр. 81 – 95. <https://journals.nauka-nanrk.kz/physics-mathematics/article/view/5414/3871>

21 Твиттер. Обновление наших правил против ненавистного поведения. 2020. https://blog.twitter.com/en_us/topics/company/2019/hatefulconductupdate.html .

22 Aggarwal & Ryoo (2011) Aggarwal JK, Ryoo MS. Human activity analysis: a review. *ACM Computing Surveys (CSUR)* 2011;43(3):16:1–16:43. doi: 10.1145/1922649.1922653. [[CrossRef](#)] [[Google Scholar](#)]

23 Poppe (2010) Poppe R. A survey on vision-based human action recognition. *Image and Vision Computing*. 2010;28(6):976–990. doi: 10.1016/j.imavis.2009.11.014. [[CrossRef](#)] [[Google Scholar](#)]

24 Sun & Liu (2013) Sun Q, Liu H. Learning spatio-temporal co-occurrence correlograms for efficient human action classification. 2013 IEEE international

conference on image processing; Piscataway. 2013. pp. 3220–3224. [CrossRef] [Google Scholar]

25 Naik & Gopalakrishna (2017) Naik AJ, Gopalakrishna MT. Violence detection in surveillance video—a survey. *International Journal of Latest Research in Engineering and Technology (IJLRET)* 2017;1:1–17. [Google Scholar]

26 Omarov B, Narynov S, Zhumanov Z, Gumar A, Khassanova M. State-of-the-art violence detection techniques in video surveillance security systems: a systematic review. *PeerJ Comput Sci.* 2022 Apr 6;8:e920. doi: 10.7717/peerj-cs.920. PMID: 35494848; PMCID: PMC9044356.

27 Mashechkin I, Petrovskiy M., Tsarev D, Chikunov M. Machine Learning Methods for Detecting and Monitoring Extremist Information on the Internet // *Programming and Computer Software.* – 2019. –Vol.45. –P.99 – 115.

28 Kotzé E., Senekal B.A., Daelemans W. Automatic classification of social media reports on violent incidents in South Africa using machine learning // *South African Journal of Science.* – 2020. –Vol.116, №3. –P.1 – 8.

29 Wu, P., Liu, J., Shen, F.: A deep one-class neural network for anomalous event detection in 1120 complex scenes. *IEEE Trans. Neural Networks Learn. Syst.* 31, 2609–2622 (2019)

30 Arandjelovic, R., Gronat, P., Torii, A., Pajdla, T., & Sivic, J. (2016). NetVLAD: CNN architecture 878 for weakly supervised place recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 5297-5307).

31 Гафаров Ф.М. Искусственные нейронные сети и приложения: учебное пособие. – Казань: Издательство Казанского университета, 2018. –С.121.

32 Zhuang, N., Yusufu, T., Ye, J., & Hua, K. A. (2017, May). Group activity recognition with differential recurrent convolutional neural networks. In *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)* (pp. 526-531). IEEE.

33 Н. Zhengbing, I. Tereykovskiy, L. Tereykovska, V. Pogorelov. Determination of structural parameters of multilayer perceptron designed to estimate parameters of technical systems // *Intelligent Systems and Applications*, 2017, 10, P. 57-62.

34 Терейковська Л. О. Методологія автоматизованого розпізнавання емоційного стану слухачів системи дистанційного навчання: дис. ... докт. техн. наук : 05.13.06. Київ. 2023. 395 с.

35 https://www.researchgate.net/publication/312336397_Preprocessing_for_image_classification_by_convolutional_neural_networks

36 Pawar K, Attar V. 2019. [Deep learning approaches for video-based anomalous activity detection](#). *World Wide Web* 22(2):571-601

37 Naik AJ, Gopalakrishna MT. 2021. [Deep-violence: individual person violent activity detection in video](#). *Multimedia Tools and Applications* 80(12):18365-18380

38 K. K. Pal and K. S. Sudeep, "Preprocessing for image classification by convolutional neural networks," in 2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), 2016, pp. 1778–1781.

39 <https://www.sciencedirect.com/science/article/pii/S0141118722003352>

40 https://www.researchgate.net/publication/365726702_Bilinear_and_Bicubic_Interpolations_for_Image_Presentation_of_Mechanical_Stress_and_Temperature_Distribution.

41 Constantin MG, Stefan LD, Ionescu B, Demarty CH, Sjoberg M, Schedl M, Gravier G. 2020. [Affect in multimedia: benchmarking violent scenes detection](#). *IEEE Transactions on Affective Computing*

42 <https://arxiv.org/pdf/1704.04861.pdf>

43 https://openaccess.thecvf.com/content_cvpr_2018/papers/Sandler_MobileNetV2_Inverted_Residuals_CVPR_2018_paper.pdf

44 <http://arxiv.org/pdf/1508.03790v2.pdf>

45 <http://arxiv.org/pdf/1402.3511v1.pdf>

46 <http://arxiv.org/pdf/1503.04069.pdf>

47 <http://jmlr.org/proceedings/papers/v37/jozefowicz15.pdf>

48 <https://arxiv.org/pdf/1704.04861.pdf>

49 Lorenzo-Navarro J., Deniz O., Santana M. C., Guerra C. Comparison of Focus Measures in Face Detection Environments // Proc. the Fourth Intern. Conf. on Informatics in Control, Automation and Robotics, Robotics and Automation 2, Angers, France, May 9–12, 2007. INSTICC Press, 2007. P. 418–423.

50 Krotkov E. Focusing // Intern. J. of Computer Vision. 1987. Vol. 1. N 3. P. 223–237.

51 Wang, Z. A universal image quality index / Z. Wang, A Bovik // IEEE Signal Processing Letters. – 2002. – V. 9, № 3, Mar. – P. 81–84.

52 Hu Z., Tereikovskiy I., Tereikovska L., Tsiutsiura M., Radchenko K. (2020) Applying Wavelet Transforms for Web Server Load Forecasting. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol 938. Springer, Cham. Pages 13-22 https://doi.org/10.1007/978-3-030-16621-2_2 [Scopus]. https://link.springer.com/chapter/10.1007/978-3-030-16621-2_2

53 Sudhakaran, S., & Lanz, O. (2017, August). Learning to detect violent videos using convolutional long short-term memory. In 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (pp. 1-6). IEEE.

54 Nievas E. B., Suarez O. D., García G. B. and Sukthankar R., "Violence detection in video using 1016 computer vision techniques", International Conference on Computer Analysis of Images and 1017 Patterns, pp. 332-339, 2011.

55 Bermejo E, Deni O, Bueno G, Sukthankar R. (2011) Violence detection in video using computer 886 vision techniques. 14th Int. Congress on Computer Analysis of Images and Patterns.

56 Xu, X., Wu, X., Wang, G., & Wang, H. (2018, December). Violent video classification based on spatial-temporal cues using deep learning. In 2018 11th International Symposium on Computational Intelligence and Design (ISCID) (Vol. 1, pp. 319-322). IEEE.

57 Xu K., Jiang X., Sun T., Anomaly detection based on stacked sparse coding with intraframe classification strategy, IEEE Transactions on Multimedia 20 (5) (2018)

58 Bermejo E, Deni O, Bueno G, Sukthankar R. (2011) Violence detection in video using computer vision techniques. 14th Int. Congress on Computer Analysis of Images and Patterns.

59 Rota, P., Conci, N., Sebe, N., & Rehg, J. M. (2015, September). Real-life violent social interaction detection. In 2015 IEEE International Conference on Image Processing (ICIP) (pp. 3456-3460). IEEE.

60 Болатбек М.А., Экстремизм түсінігі. Экстремистік мәтіндерді анықтауға арналған белгілер жинағына шолу // Международная научная конференция студентов и молодых ученых «Фараби әлемі». –Алматы: Қазақ университеті, 2020.

61 Болатбек М.А. Экстремистік мәтіндерді сентимент талдау арқылы анықтау // Международная научная конференция студентов и молодых ученых «Фараби әлемі». –Алматы: Қазақ университеті, 2020. –Б. 75–76.

62 Tukeyev U., Turganbayeva A., Abduali B., Rakhimova D., Amirova D., Karibayeva A. Lexicon-free stemming for Kazakh language information retrieval. // IEEE 12th International Conference on Application of Information and Communication Technologies (AICT).–Almaty, 2018.–P.1–4.

63 Мусиралиева Ш.Ж., Болатбек М.А., Зият Б.М. Стемминг алгоритмі арқылы экстремистік мәтіндерді жіктеу дәлдігін арттыру // ҚазҰТЗУ хабаршысы. – 2020. №6 (142).–Б.208–215.

64 Мусиралиева Ш.Ж., Болатбек М.А. Әлеуметтік желідегі экстремистік мәтіндерді жіктеу дәлдігін грамматикалық қателерді анықтау және түзету арқылы арттыру // Международная научно-практическая конференция «Актуальные проблемы информационной безопасности в Казахстане».–Алматы, 2020.–Б.57–61.

65 М.А. Болатбек, К.Б. Багитова, Ш.Ж. Мусиралиева. Киберқауіпсіздік мәселелерін табиғи тілді өңдеу әдістері арқылы шешу тақырыбына жүйелік шолу. NEWS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN PHYSICO-MATHEMATICAL SERIES ISSN 1991-346X VOLUME 3, NUMBER 343 (2022), 52-70. <https://journals.nauka-nanrk.kz/physics-mathematics/article/view/4690/3560>

66 М.А. Болатбек, Ш.Ж. Мусиралиева, К. Багитова, А.Т.Нюсупов, Е. Абайұлы. Веб-ресурстардағы фишингтік хабарламалар және оларды машиналық оқыту әдістері арқылы анықтау. NEWS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN PHYSICO-MATHEMATICAL SERIES ISSN 1991-346X Volume 4, Number 344 (2022), 16-29. <https://journals.nauka-nanrk.kz/physics-mathematics/article/view/4789/3655>

67 Lorenzo-Navarro J., Deniz O., Santana M. C., Guerra C. Comparison of Focus Measures in Face Detection Environments // Proc. the Fourth Intern. Conf. on Informatics in Control, Automation and Robotics, Robotics and Automation 2, Angers, France, May 9–12, 2007. INSTICC Press, 2007. P. 418–423.

68 Mussiraliyeva, S., Bolatbek, M., Omarov, B., Bagitova, K. Detection of Extremist Ideation on Social Media Using Machine Learning Techniques. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020, 12496 LNAI, стр. 743–752 (scopus indexed, процентиль 50) https://link.springer.com/chapter/10.100/978-3-030-63007-2_58 12th International Conference, ICCCI 2020, Da Nang, Vietnam, November 30 – December 3, 2020, Proceedings

69 Ш.Ж. Мусиралиева, К.Б. Багитова, И.А. Терейковский, А.М. Усманова. Әлеуметтік желілердегі суреттер мен бейнелерді өңдеудің ерекшеліктері VIII - международная научно-практическая конференция «Информатика и прикладная математика», 26-27 октября 2023 года, Алматы, Казахстан, 305 – 310 стр.

70 Wang, Z. A universal image quality index / Z. Wang, A Bovik // IEEE Signal Processing Letters. – 2002. – V. 9, № 3, Mar. – P. 81–84.

71 Hu Z., Tereikovskiy I., Tereikovska L., Tsiutsiura M., Radchenko K. (2020) Applying Wavelet Transforms for Web Server Load Forecasting. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing, vol 938. Springer, Cham. Pages 13-22 https://doi.org/10.1007/978-3-030-16621-2_2 [Scopus]. https://link.springer.com/chapter/10.1007/978-3-030-16621-2_2

72 K. Bagitova, I. Tereikovskiy, I. Babayev, L. Tereikovska, O. Tereikovskiy. Model for processing images of online social networks used to recognize political extremism. Journal of Mathematics, Mechanics and Computer Science. Vol. 119 No. 3 (2023): Journal of Mathematics. P. 91-103. ISSN 1563–0277, eISSN 2617-4871 DOI: <https://doi.org/10.26577/JMMCS2023v119i3a8>
<https://bm.kaznu.kz/index.php/kaznu/article/view/1321>

73 Galassi, A., Lippi, M., & Torroni, P. (2021). Attention in Natural Language Processing. IEEE Transactions On Neural Networks And Learning Systems, Vol. 32, No. 10. <https://doi.org/10.1109/TNNLS.2020.3019893>

74 S. Toliupa, I. Tereikovskiy, L. Tereikovska, S. Mussiraliyeva and K. Bagitova, "Deep Neural Network Model for Recognition of Speaker's Emotion," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 172-176, doi: 10.1109/PICST51311.2020.9468017. <https://ieeexplore.ieee.org/document/9468017>

75 Brauwera, G., & Frasinca, F. (2021). A General Survey on Attention Mechanisms in Deep Learning. IEEE Transactions on Knowledge and Data Engineering (TKDE). <https://doi.org/10.1109/TKDE.2021.3126456>

76 Rothman, D. (2022). Transformers for Natural Language Processing: Build, train, and fine-tune deep neural network architectures for NLP with Python, PyTorch, TensorFlow, BERT, and GPT-3, 2nd Edition. Packt Publishing

77 Mussiraliyeva S., Omarov B., Bolatbek M., Bagitova K., Alimzhanova Z. (2021) Bigram Based Deep Neural Network for Extremism Detection in Online User Generated Contents in the Kazakh Language. 13th International Conference, ICCCI 2021, Rodos, Greece, October 2021. Advances in Computational Collective Intelligence. ICCCI 2021. vol 1463, pp 743-752. Springer, Cham. https://doi.org/10.1007/978-3-030-88113-9_45

78 Shynar Mussiraliyeva, Kalamkas Bagitova and Daniyar Sultan, “Social Media Mining to Detect Online Violent Extremism using Machine Learning Techniques” International Journal of Advanced Computer Science and Applications(IJACSA), 14(6), 2023. <http://dx.doi.org/10.14569/IJACSA.2023.01406146>

79 Ye, L., Wang, P., Wang, L., Ferdinando, H., Seppänen, T., & Alasaarela, E. (2018). A combined motion-audio school bullying detection algorithm. International Journal of Pattern Recognition and Artificial Intelligence, 32(12).

80 Accattoli, S., Sernani, P., Falcionelli, N., Mekuria, D. N., & Dragoni, A. F. (2020). Violence detection in videos by combining 3D convolutional neural networks and support vector machines. Applied Artificial Intelligence, 34(4), 329-344.

81 Al-Nawashi, M., Al-Hazaimh, O. M., & Saraee, M. (2017). A novel framework for intelligent surveillance system based on abnormal human activity detection in academic environments. Neural Computing and Applications, 28(1), 565-572.

82 K. Bagitova, I. Tereikovskiy, I. Babayev, L. Tereikovska, O. Tereikovskiy. Model for processing images of online social networks used to recognize political extremism. DOI: <https://doi.org/10.26577/JMMCS2023v119i3a8> Vol. 118 No. 2 (2023): Journal of Mathematics, Mechanics and Computer Science (**indexed in Web of Science**).

83 Arandjelovic, R., Gronat, P., Torii, A., Pajdla, T., & Sivic, J. (2016). NetVLAD: CNN architecture for weakly supervised place recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 5297-5307).

84 Auria, L., & Moro, R. (2007). Advantages and disadvantages of support vector machines. Credit Risk Assessment Revisited: Methodological Issues and Practical Implications, 49-68.

85 Bas, P., Filler, T., & Pevný, T. (2011, May). ” Break our steganographic system”: the ins and outs of organizing BOSS. In International workshop on information hiding (pp. 59-70). Springer, Berlin, Heidelberg.

86 Bermejo E, Deni O, Bueno G, Sukthankar R. (2011) Violence detection in video using computer vision techniques. 14th Int. Congress on Computer Analysis of Images and Patterns, pp. 332-339. Benchmarking violent scenes detection in movies. In: 2014 12th International Workshop on Content-Based Multimedia Indexing (CBMI), pp. 1–6. IEEE (2014)

87 Deviatkin D., Smirnov I., Solovyev F., Suvorova M., Chepovskiy A. Extremist Text Detection In Social Web // Multi Conference on Computer Science and Information Systems, MCCSIS 2019. –Porto, 2019. –P.344–350.

88 Ананьева М.И., Девяткин Д.А., Кобозева М.В., Смирнов И.В. Лингвостатистический анализ текстов экстремистской направленности // Ситуационные центры и информационно-аналитические системы класса 4i для задачи мониторинга и безопасности (SCVRT2015-16). Том 1, 2016. –С.210–213.

89 Ананьева М. И., Кобозева М. В., Соловьев Ф. Н., Поляков И. В., Чеповский А. М. О проблеме выявления экстремистской направленности в текстах // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2016. Том 14, № 4. –С.5–13.