ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ІШКІ ІСТЕР МИНИСТРЛІГІ

МАҚАН ЕСБОЛАТОВ АТЫНДАҒЫ
АЛМАТЫ АКАДЕМИЯСЫ

ӘЛЕУМЕТТІК ОРТАДАҒЫ ПАЙДАЛАНУШЫЛАРДЫ ДЕАНОМИЗАЦИЯЛАУДЫҢ ЗАМАНАУ ӘДІСТЕРІН ЗЕРТТЕУ

Әдістемелік ұсыным

Алматы
2025

Қазақстан Республикасы Ішкі істер министрлігі М. Есболатова атындағы Алматы академиясының ғылыми-әдістемелік кеңесінің отырысында талқыланды және бекітілді (2025 жылғы 15 мамырдағы №5 хаттама).

Рецензенттер:

Байшоланова Қ.С. – Әл-Фараби атындағы Қазақ ұлттық университетінің профессоры, экономика ғылымдарының докторы.

Қалдыбаев А.Б. – Алматы қалалық ПД Киберқылмыспен күрес басқармасының бастығы полиция полковнигі .

Кадырова Р.Т., Уралова Ф.С., Суюнбай Ж.: Әлеуметтік ортадағы пайдаланушыларды деанонимизациялаудың заманауи әдістерін зерттеу: Әдістемелік ұсыным. – Алматы: Қазақстан Республикасы ІІМ М. Есболатова атындағы Алматы академиясының ҒЗҰжРБЖҰБ, 2025. – 40 б.

Әдістемелік ұсыным әлеуметтік ортадағы пайдаланушыларды деанонимизациялау мәселелеріне арналған және Интернет кеңістігінде жеке басын жасыратын тұлғаларды анықтау үшін қолданылатын қазіргі әдістерді ашады. OSINT, стилистикалық мәтін талдауы, цифрлық ізді талдау және мінез-құлық талдауы үшін машиналық оқыту әдістері сияқты технологияларға ерекше назар аударылады. Жұмыс кең ауқымды зерттеушілерге, ғалымдар мен қызметкерлерге, сондай-ақ құқық қорғау органдарының жоғары оқу орындарының курсанттарына, тыңдаушыларына, магистранттарына және докоранттарына арналған.

Кіріспе

Соңғы жылдары цифрлық кеңістікте, әсіресе Telegram сияқты платформаларда анонимді белсенділіктің күрт өсуі байқалды. Мұндай коммуникацияларға қатысушылар жалған аккаунттарды, боттарды және күдікті ресурстарға әкелетін сілтемелерді пайдалану арқылы өздерінің жеке басын жасырады. Бұл пайдаланушы қауіпсіздігіне қауіп төндіреді және зиянкестерді тиімді анықтауға жол бермейді. Мұндай жағдайларда анонимизациялаудың заманауи әдістерін – олардың мінез-құлқы мен цифрлық іздерін талдау негізінде анонимді пайдаланушыларды сәйкестендіруге мүмкіндік беретін құралдарды әзірлеу және енгізу ерекше маңызға ие.

Машиналық оқыту технологияларын, табиғи тілді өңдеу (NLP) және OSINT (ашық бастапқы интеллект) әдістерін пайдалану [21] пайдаланушы әрекеттері арасындағы жасырын үлгілер мен корреляцияларды анықтай отырып, мәтінді автоматты өңдеудің жаңа мүмкіндіктерін ашады. Контейнер архитектурасын (Docker) қолданумен бірге бұл тәсілдер нақты уақытта жұмыс істейтін және талдаудың жоғары дәлдігіне ие икемді жүйелерді құруға мүмкіндік береді.

Бұл әдістемелік ұсыныстар студенттердің әлеуметтік желідегі қолданушылардың мінез-құлқын талдау және олардың ықтимал сәйкестігін анықтау үшін цифрлық технологияларды қолданудағы теориялық білімдері мен практикалық дағдыларын дамытуға бағытталған. Құжат онлайн анонимділіктің тұжырымдамалық аспектілерін де, қолданбалы шешімдерді енгізуді де қамтиды: деректерді жинаудан аналитикалық модельдерді құруға және нәтижелерді визуализациялауға дейін.

Ұсыныстар курсанттарға, магистранттарға, тыңдаушыларға, сондай-ақ ақпараттық қауіпсіздік, сандық криминалистика және интернет деректерін талдау саласындағы мамандарға арналған.)

1 Деанонимизацияның теориялық негіздері сандық платформалардағы пайдаланушылар

Деанонимизация – әдейі немесе әдепкі бойынша цифрлық кеңістікте өзінің жеке басын жасыратын пайдаланушының жеке басын анықтау процесі. Әлеуметтік желілер мен мессенджерлердің қарқынды дамуы жағдайында бұл концепция әсіресе анонимді әрекетке қатысты оқиғалардың көбеюіне байланысты өзекті болып отыр. Интернеттегі анонимділік әртүрлі формаларда көрінуі мүмкін:

– Техникалық анонимдік – VPN, прокси және Tor арқылы IP мекенжайыңызды және басқа желі параметрлерін жасыру.

– Бүркеншік ат – нақты деректердің орнына жалған есімдерді, бүркеншік аттарды немесе аватарларды қолдану.

– Мінез-құлық анонимділігі – пайдаланушыны анықтауға болатын мінез-құлықтың бірегей үлгілерін қалдырмау ниеті.

– Контентті анонимділігі – бұл адамның жеке басын ашпайтын ақпаратты орналастыру (мысалы, анонимді хабарламалар, EXIF деректері жоқ суреттер және т.б.).

Деанонимдеу процедуралары нақты субъектінің жеке басын ашуға да, бір пайдаланушының аккаунттары арасындағы байланысты анықтауға да бағытталуы мүмкін. Бұл тәсілдер сандық іздерді талдауға негізделген – пайдаланушы Интернет ресурстарымен әрекеттесу кезінде қалдыратын ақпарат жиынтығы. Деанонимизацияның негізгі бағыттары:

– мінез-құлық және уақытша үлгілерді талдау,

– мәтіндерге стилистикалық сараптама (стилометрия),

– әртүрлі көздерден алынған деректерді салыстыру (платформалық корреляция),

– әлеуметтік байланыстарды визуализациялау.

Қазіргі деанонимизация әдістері көбінесе машиналық оқыту мен OSINT мүмкіндіктерін біріктіреді [37] [38],

ақпаратты автоматтандырылған жинауға, салыстыруға және интерпретациялауға мүмкіндік береді.

Осылайша, деанонимизация киберқауіпсіздік, лингвистика, мінез-құлық талдауы және цифрлық сот сараптамасы салаларындағы білімді біріктіретін пәнаралық сала болып табылады.

1.1 Цифрлық ортадағы анонимділіктің түсінігі мен түрлері

Цифрлық ортадағы анонимдік – бұл пайдаланушының жеке басын байланысқа қатысушылардың немесе техникалық құралдардың көмегімен тікелей немесе сенімді түрде анықтау мүмкін емес күй. Бұл құбылыс заманауи Интернеттің ажырамас бөлігі болып табылады және оны оң жағынан да – жеке өмірге қол сұғылмаушылық пен сөз бостандығын қорғау тұрғысынан да, теріс жағынан да – құқықтарды, қауіпсіздікті бұзу және заңсыз әрекеттерді жүзеге асыру тұрғысынан қарауға болады.

Цифрлық анонимдік технологиялық, мінез-құлық және құқықтық факторлардың қиылысында қалыптасады. Пайдаланушылар өздерінің жеке басын әдейі жасыра алады, мысалы, бүркеншік аттарды, мамандандырылған сәйкестендіруді айналып өту құралдарын (VPN, Tor, прокси серверлер) пайдалану арқылы немесе байқаусызда – жай ғана цифрлық қызметтермен әрекеттесу кезінде нақты жеке деректерді бермеу. Мотивке қарамастан, анонимдік субъект туралы ақпараттың қолжетімділік деңгейі қатаң шектелген жағдайды білдіреді.

Жеке басын жасыру әдісі мен тереңдігімен ерекшеленетін анонимдіктің бірнеше негізгі түрлері бар. Техникалық анонимділік пайдаланушының желі параметрлерін бүркемелейтін құралдарды пайдалануға негізделген. Бұл шешімдер IP мекенжайын, геолокацияны, құрылғы ақпаратын және басқа сандық идентификаторларды жасыруға мүмкіндік береді.

Бұған трафикті аралық серверлер арқылы бағыттау, қосылымдарды шифрлау және cookie файлдарын жою арқылы қол жеткізіледі. Дегенмен, техникалық қорғаудың жоғары деңгейінің өзінде мінез-құлық деректерін салыстыру арқылы жанама сәйкестендіру мүмкіндігі сақталады.

Бүркеншік ат – әлеуметтік платформалардағы анонимдіктің ең көп таралған түрі. Пайдаланушы өзінің нақты тұлғасын көрсетпей-ақ жалған атпен немесе лақап атпен әрекет ете алады. Бұл ретте тіркелгі мен өзара әрекеттесу тарихы тұрақты болып қалады, бұл тұрақты цифрлық кескінді қалыптастыруға мүмкіндік береді. Бүркеншік ат анонимдеу мүмкіндігін жоққа шығармайды, әсіресе тіркелгі басқа тіркелгілерге байланыстырылған немесе жеке ақпарат элементтері бар жағдайларда.

Мінез-құлық анонимділігі пайдаланушының цифрлық кеңістіктегі әрекеттерінің сипаттамаларына қатысты. Әр адамның ақпараттық жүйелермен өзара әрекеттесуінің өзіндік стилі бар: хабарлама жазу ырғағы, типтік қателер және белсенділік уақытындағы қалаулар. Бұл мүмкіндіктер адамның сандық саусақ ізі ретінде пайдаланылуы мүмкін және оларды машиналық оқыту әдістері арқылы талдауға болады. Аты, IP мекенжайы немесе басқа тікелей көрсеткіштері болмаса да, мінез-құлық ізі белгілі бір адамға немесе топқа нұсқауы мүмкін.

Мазмұнның анонимділігі хабарды құрастыру стилінде, сөздерді таңдауда, қарым-қатынас тақырыбы мен контекстінде көрінеді. Стилометриялық талдау мәтіннің авторын анықтауға немесе тілдік ерекшеліктеріне қарай бірнеше хабарламаларды бір-бірімен байланыстыруға мүмкіндік береді. Бұл тәсіл әсіресе автор өзінің қатысуын жасыруға тырысатын әлеуметтік желілердегі жасырын аккаунттарды ашу үшін өте өзекті.

Соңында, желі анонимділігі тіркелгілер арасындағы құрылымдық қатынастар тұрғысынан қарастырылады. Арнайы пайдаланушылар жеке ақпаратты ашпаса да, олардың байланыстары, жазылымдары, топқа қатысуы және басқа

тіркелгілермен қиылысулары әлеуметтік желіні құру үшін талдауға болады. Графикалық әдістер мен қауымдастықтарды анықтау алгоритмдері анонимді пайдаланушының белгілі бір топқа немесе тіпті белгілі бір адамға қатыстылығын анықтауға мүмкіндік береді .

Осылайша, цифрлық ортадағы анонимділік деректерді жасырудың техникалық аспектілерін ғана емес, сонымен қатар мінез-құлық, лингвистикалық және желілік сипаттамаларды қамтитын көп қырлы құбылыс болып табылады. Анонимділіктің түрлері мен деңгейлерін түсіну тиімді деанонимизация әдістерін әзірлеу және ақпараттық қауіпсіздік тәуекелдерін бағалау үшін қажет. Анонимділіктің абсолютті емес екенін ескеру ерекше маңызды: егер деректердің жеткілікті мөлшері және тиісті аналитикалық құралдар болса, оны жеке ақпаратқа тікелей қол жеткізуге жүгінбей бұзуға болады [39].

1.2 Әлеуметтік платформалар орта ретінде анонимді әрекет

Заманауи әлеуметтік платформалар пайдаланушыларға коммуникация, өзін-өзі сәйкестендіру, мазмұнды тарату және цифрлық қауымдастықтарды қалыптастыру үшін бірегей мүмкіндіктер береді. Сонымен қатар, дәл осы платформалар анонимді әрекетке, соның ішінде құқықтарды бұзуға, жалған ақпарат таратуға және басқа да ықтимал қауіпті әрекеттерге арналған кеңістікке айналуда. Пайдаланушыға ұсынылатын анонимдік дәрежесі платформа архитектурасына, құпиялылық саясатына және модерация деңгейіне байланысты өзгереді [2][3].

Әлеуметтік желіде анонимділіктің танымал болуының негізгі себептерінің бірі – қудалаудан, стигматизациядан немесе цензурадан қорықпай өз ойларын еркін жеткізу мүмкіндігі. Дегенмен, анонимдіктің жоғары дәрежесі заңсыз мақсаттарда жиі қолданылады: зиянды ақпаратты таратқанда

жеке басын жасыру, заңсыз әрекеттерді үйлестіру немесе қоғамдық кеңістікті манипуляциялау [9].

Анонимді әрекеттің мүмкіндіктерін талдау үшін платформалардың әртүрлі түрлерін қарастырған жөн (1-сурет) пайдаланушыны сәйкестендіру критерийлеріне, жеке деректердің қолжетімділігіне және әкімшілік тарапынан бақылау деңгейіне негізделген.

Платформа	Регистрация с номером/почтой	Возможность использования псевдонима	Отображение username	Уровень модерации	Условие деанонимизации
Telegram	Да (телефон)	Да	Да	Низкий	Через OSINT, поведенческий анализ
Reddit	Электронная почта	Да	Да	Средний	Через историю постов и IP
Twitter (X)	Да (почта/телефон)	Да	Да	Средний/высокий	Анализ сети связей, лексики
4chan	Нет	Да (анонимно)	Нет	Очень низкий	Почти невозможна
Facebook	Да (настоящее имя по правилам)	Нет	Да	Высокий	Высокая вероятность

1-сурет. Танымал платформалардағы анонимділік шарттары

1-суретте көрсетілгендей, Telegram және Reddit платформалары пайдаланушыларға жеке сәйкестендіруге қойылатын минималды талаптарға және тіркелгіні қатаң тексерудің болмауына байланысты анонимділіктің жоғары деңгейін сақтау мүмкіндігін береді. Бұл мұндай платформаларды өздерінің жеке басын жасырғысы келетін адамдар үшін тартымды етеді. Сонымен қатар, қатаң модерацияның жоқтығы және бүркеншік аттарды қолдану мүмкіндігі хабарлар көзін немесе аккаунттың нақты иесін анықтау процесін қиындатады [5].

Telegram – шартты анонимділігі бар платформаның ең көрнекті мысалдарының бірі. Телефон нөмірі бойынша міндетті тіркеуге қарамастан, нөмірдің өзі басқа

пайдаланушылардан жасырылуы мүмкін және сәйкестендіру көбінесе бүркеншік атпен шектеледі. Сонымен қатар сыртқы құралдардың көмегімен – Telegram API, OSINT талдауы, ашық топтарды талдау – қолданушының мінез-құлық профилін құруға және қайталанатын белсенділік белгілерін анықтауға болады [40].

Басқа шеткі жерде Facebook сияқты платформалар бар, мұнда «шын есім» саясаты анонимділіктің төмен деңгейін жасайды. Барлық пайдаланушылар бұл ережелерді іс жүзінде орындамаса да, модерация және жалған тіркелгіні анықтау алгоритмдері анонимді әрекетті әлдеқайда қиындатады.

Фактор	Описание	Влияние
Наличие обязательной верификации	Требование подтверждения личности или телефона	Снижает
Возможность скрыть метаданные	Прямое или косвенное отображение ID, IP, геолокации	Повышает
Публичность профиля	Доступность истории сообщений и активности	Снижает
Интеграция с другими сервисами	Возможность сопоставления данных с другими платформами	Снижает
Политика модерации	Активное удаление подозрительного или вредоносного контента	Снижает
Возможность использования ботов	Применение автоматических аккаунтов без привязки к личности	Повышает

2-сурет. Анонимдік дәрежесіне әсер ететін факторлар

Талдау көрсеткендей, жасырындық деңгейі платформаның құрылымына ғана емес, сонымен қатар пайдаланушының мінез-құлқына да байланысты. Шектеулі сәйкестендіру жағдайында да цифрлық іздер – белсенділік уақыты, хабарламалар құрылымы, қолданылатын сөздік түріндегі – сәйкес талдау құралдары болған жағдайда сәйкестікті анықтау үшін пайдаланылуы мүмкін [6] [14].

Осылайша, әлеуметтік платформалар құпиялылықты қамтамасыз ету құралы ретінде де, жасырындықты теріс пайдалану нақты қауіптерге әкелуі мүмкін кеңістік ретінде де қызмет етеді. Анонимділікке әсер ететін механизмдерді түсіну, әсіресе ақпараттық қауіпсіздік, сандық криминалистика және ашық бастапқы деректер мониторингі контекстінде деанонимизация әдістерін дамытудың кілті болып табылады.

2 Әдістер мен құралдар пайдаланушы идентификациясы

Деанонимдеу мәселелерін шешу үшін мәтінді өңдеудің заманауи әдістері, машиналық оқыту және ашық бастапқы интеллект (OSINT) қолданылады. Бұл тәсілдер мінез-құлқы, тілі және цифрлық іздері негізінде жеке басын жасыратын пайдаланушыларды анықтауға мүмкіндік береді.

Табиғи тіл өңдеу (NLP) технологиялары [4] мәтін құрылымын, жазу стилін және қайталанатын өрнектерді талдау үшін қолданылады. Бұл бір автордың әртүрлі тіркелгілері арасында байланыс орнатуға немесе хабарлардағы ауытқуларды анықтауға көмектеседі.

Random Forest және BERT сияқты машиналық оқыту үлгілері хабарламаларды автоматты түрде жіктеу және олардың анонимді сипатын бағалау үшін пайдаланылады. Бұл әдістер күдікті хабарламаларды анықтауға және мінез-құлық талдауын жүргізуге мүмкіндік береді [7].

Ашық бастапқы интеллект (OSINT) пайдаланушы атын, уақыт белгілерін, әрекетті және пайдаланушылар арасындағы қарым-қатынастарды талдауды қамтиды. Мұндай деректер анонимді қатысушының шынайы тұлғасы туралы гипотеза жасауға мүмкіндік береді.

Жүйенің барлық құрамдас бөліктері икемділікті, қайталануды және кейінгі талдау үшін ыңғайлы интеграцияны қамтамасыз ететін Docker контейнерлерінің көмегімен жүзеге асырылады.

2.1 OSINT және ашық деректерді талдау

Заманауи ақпараттық кеңістікте ашық бастапқы интеллект (OSINT) – бұл жалпыға қолжетімді және заңды түрде қол жетімді деректерді жинау және талдаудың жүйелі тәсілі. OSINT пайдалану деанонимдеу тапсырмаларындағы негізгі әдістердің бірі болып табылады, өйткені ол пайдаланушыны бұзу немесе жабық жүйелерге рұқсатсыз кіруді қолданбай, оның сандық іздерінің жиынтығы негізінде анықтауға мүмкіндік береді.

OSINT талдауы көп арналы ақпаратты салыстыру принципіне негізделген: пайдаланушы бір қызметте өзінің жеке басын белсенді түрде бүркемелесе де, оның басқа көздердегі (форумдардағы, әлеуметтік желілердегі, дерекқорлардағы, жалпыға қолжетімді API интерфейстеріндегі) белсенділігі идентификациялық мүмкіндіктерді байқаусызда ашуы мүмкін. OSINT талдау кезеңдері [13] :

– Зерттеу мақсаттарын анықтау – тапсырма тұжырымдалады: сәйкестікті орнату, шоттардың арасындағы байланысты табу, деректердің шынайылығын тексеру және т.б.

– Бастапқы ақпаратты жинау Telegram API, іздеу операторлары, ағып кету агрегаторлары, мамандандырылған OSINT платформалары (мысалы, Spiderfoot, Maltego, Recon-ng) арқылы жүзеге асырылады.

– Деректерді талдау және сүзу – алынған деректер көшірмелерден тазартылады және түрі бойынша жіктеледі (пайдаланушы аты, электрондық пошта, IP, телефон, уақыт белгісі және т.б.).

– Қарым-қатынастарды құру – графикалық талдауды қолдану арқылы тіркелгілер, қызметтер және пайдаланушы әрекеттері арасындағы қарым-қатынастар анықталады.

– Нәтижелерді интерпретациялау және құжаттау – визуализацияларды, анықтамаларды және интерпретацияларды қамтитын есеп жасалады.

Источник	Тип данных	Применение
Telegram API	Username, ID, сообщения, дата	Идентификация активности, временные паттерны
Google Search / Dorks	Имя, email, сайты, утечки	Сопоставление аккаунтов, поиск следов по никнейму или email
Maltego	Связанные сущности, профили	Визуализация связей между учетными записями
ExifTool	Метаданные изображений	Извлечение координат, устройств, времени съемки
HavelBeenPwned, LeakCheck	Базы утечек	Поиск совпадений по email, логинам
GitHub, Reddit, Twitter	Контент, стиль, активность	Кросс-платформенный анализ поведения и стиля

3-сурет. Анонимизация тапсырмаларындағы OSINT деректер көздерінің мысалдары [1]

OSINT талдауын қолданудың мысалы Telegram-да табылған бүркеншік атпен жұмыс істеу болып табылады. Пайдаланушы аты арқылы зерттеуші операторларды («пайдаланушы аты» site: twitter.com) пайдаланып Google-да автоматтандырылған іздеу жүргізе алады, дерекқорлардағы ағып кетуді тексеріп, әртүрлі қызметтердегі жарияланымдардың уақыты мен стилін талдай алады. Егер пайдаланушы бірнеше платформаларда бір лақап атын қалдырса, бір цифрлық профильді орнату мүмкін болады.

Сонымен қатар, мультимедиялық контент – фотосуреттер, дауыстық хабарламалар болған жағдайда – метадеректерді талдау және лингвистикалық сараптама әдістері қолданылады. Мысалы, кескінде нақты координаттары, құрылғы үлгісі және жасалған уақыты бар EXIF ақпараты болуы мүмкін.

Осылайша, OSINT [22] [23] классикалық деанонимизация әдістерін толықтырып қана қоймайды, сонымен қатар сандық сәйкестендірулерді өздігінен анықтау және қадағалаудың қуатты құралы ретінде қызмет етеді. Оның

тиімділігі қол жетімді деректер көлемімен ғана емес, сонымен қатар талдаушының байланыстарды түсіндіру және бір-бірінен айырмашылығы бар ақпарат көздері арасындағы тривиальды емес тәуелділіктерді анықтау қабілетімен анықталады.

2.2 Машиналық оқыту технологиялары және деанонимизациядағы NLP

Қазіргі деанонимизация әдістері барған сайын машиналық оқыту (ML) және табиғи тілді өңдеу (NLP) құралдарына сүйенеді [8]. Бұл технологиялар мәтіндік және мінез-құлық деректерінің үлкен массивтерін тиімді талдауға, бірегей пайдаланушы сипаттамаларын анықтауға және анонимді цифрлық профильдер арасындағы байланыстарды қалпына келтіруге мүмкіндік береді. ML және NLP қолдану анонимді әрекет фактісін жазып қана қоймай, сонымен қатар пайдаланушының немесе ол жататын топтың ықтимал сәйкестігі туралы гипотезаларды алға тарта алатын интеллектуалды жүйелерді құруға көмектеседі [12].

1. Деанонимизация тапсырмаларындағы машиналық оқытудың рөлі

Машиналық оқыту – бұл нақты бағдарламаланбай, болжау немесе шешім қабылдау үшін тарихи деректер бойынша алгоритмдер оқытылатын жасанды интеллект саласы. Деанонимизация контекстінде ML мыналар үшін қолданылады:

– күдіктілік дәрежесіне қарай хабарламалар мен пайдаланушылардың мінез-құлқын жіктеу;

– әр түрлі шоттардың бір субъектіге жату ықтималдығын анықтау;

– цифрлық белсенділіктегі ауытқуларды анықтау;

– белгілі бір пайдаланушыларға ғана тән мінез-құлық немесе сөйлеу үлгілерін тану.

Классификациялық есептердегі кең таралған алгоритмдердің бірі - Random Forest. Бұл шешім ағаштарының

жиынтығын құруға негізделген ансамбль әдісі, онда түпкілікті нәтиже дауыс беру арқылы анықталады. Ол кестелік деректермен жұмыс істегенде жоғары дәлдікті көрсетеді, бұл оны векторлық кескінде мәтіндерді талдау үшін пайдалы етеді (мысалы, TF-IDF қолданғаннан кейін). Бұл жұмыста Random Forest моделі Telegram-дан алынған мәтіндерді анонимді әрекетке тән белгілер бойынша жіктеу үшін пайдаланылды: сілтемелердің болуы, стиль, кілт сөздер және жарияланым уақыт аралығы [24] [25].

Мәтінді тереңірек түсінуге қол жеткізу үшін Transformers нейрондық желісінің қос бағытты кодтаушы өкілдіктері (BERT) сияқты күрделі және контекстке сезімтал модельдер пайдаланылады. BERT сөйлемдегі әрбір сөздің контекстін ескере алады, бұл оны әсіресе әлеуметтік медиа мен хабар алмасу қолданбаларына тән қысқа хабарларды талдау үшін пайдалы етеді. Мұндай модельдер хабарламаларды жіктеуге ғана емес, сонымен қатар оларды кластерлеуге, нысандарды (аттар, атаулар, орындар) шығаруға және мазмұнды семантикалық талдауға мүмкіндік береді.

2. Стильді талдау және авторлықты анықтау үшін NLP пайдалану

Табиғи тіл өңдеу (NLP) – лингвистика, информатика және жасанды интеллект біріктірілген сала. Ол хабарламаларды машинамен «оқуға» және олардан маңызды ақпаратты алуға мүмкіндік беретін мәтінді талдау әдістерін қамтиды. Деанонимизация тапсырмаларында стилометрия ерекше маңызға ие – мәтін авторын анықтауға бағытталған жазу стилін талдау [15] [26].

Әрбір адам ниетіне қарамастан белгілі бір сөздік, сөйлем құрылымы, тыныс белгілері, синтаксистік айналымдарды қолданады. Бұл параметрлерді сандық түрде анықтауға және авторлық модельді құруда мүмкіндіктер ретінде пайдалануға болады. Мысалы, сөйлеудің белгілі бір бөліктерін қолдану жиілігін, сөз ұзындығын, қысқартулар мен эмодзилерді пайдалануды және жазу ырғағын (уақыт белгілері бар болса)

талдау пайдаланушының бірегей тілдік профилін жасай алады.

NLP сонымен қатар атаулы нысанды тану (NER), яғни мәтіндегі атауларды, ұйымдарды және географиялық нысандарды тану үшін қолданылады. Бұл ақпарат пайдаланушы сөйлесетін контекстті, олар не туралы жазып жатқанын және мәтінде жеке ақпарат бар-жоғын анықтауға көмектеседі. Мұндай әдістерді қолдану хабарламаларды талдауға ғана емес, сонымен қатар пайдаланушы әдейі немесе кездейсоқ қалдырған өзін-өзі анықтаудың ықтимал белгілерін анықтауға мүмкіндік береді [27] [28].

3. ML және NLP-ті бір аналитикалық жүйеге біріктіру

Машиналық оқыту және NLP үлгілерінің интеграциясы толық талдау циклін орындай алатын қуатты аналитикалық платформаны құруға мүмкіндік береді: өңделмеген мәтіндерді өңдеуден нәтижелерді визуализациялауға және есептерді шығаруға дейін. Бұл жұмыстың бір бөлігі ретінде келесі процесс жүзеге асырылды [29] [30]:

– Деректерді жинау: API арқылы Telegram-дан хабарламаларды, соның ішінде мәтінді, күнді, пайдаланушы аты, user_id шығарып алыңыз.

– Алдын-ала өңдеу: мәтінді қажетсіз таңбалардан тазарту, токенизация, нормалау, лемматизация.

– Ерекшелік: мәтіндерді векторлық кескінге түрлендіру (TF-IDF, ендіру), мінез-құлық ерекшеліктерін шығару (жіберу уақыты, жиілігі, ұзындығы).

– Жіктеу: Белсенділік санатын анықтау үшін Random Forest және BERT үлгілерін пайдалану.

– Авторлық стиль: бірегей лингвистикалық сипаттарды анықтау үшін қосымша NLP талдауы.

– Көрнекілігі: талдау нәтижелерін веб-интерфейсте көрсету (мысалы, кестелер, графиктер, жылу карталары түрінде).

Бұл тәсіл анонимді пайдаланушыларды жүйелі түрде сәйкестендіруге, сандық мінез-құлық үлгілерін қадағалауға

және киберқауіпсіздік, тергеулер немесе бұзушылықтарды бақылау үшін пайдалы профильдер құруға мүмкіндік береді.

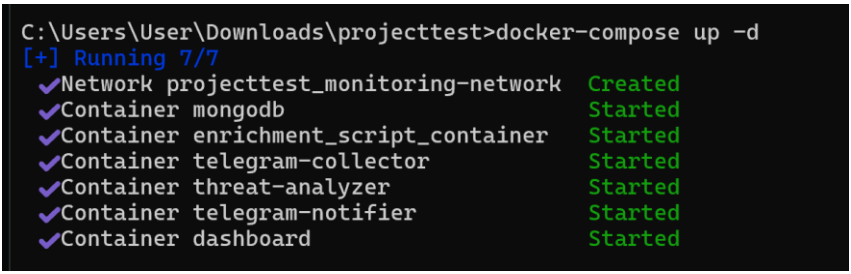
Машиналық оқыту және табиғи тілді өңдеу деанонимизацияның заманауи тәсілдерінде орталық рөл атқарады. Оларды пайдалану икемділік пен ауқымдылықты сақтай отырып, қолмен талдаудан цифрлық деректерді автоматтандырылған интерпретациялауға көшуге мүмкіндік береді. Мәтіндерді, мінез-құлық сипаттамаларын және желілік белсенділікті кешенді талдау пайдаланушының цифрлық ізін толық түсінуді қамтамасыз етеді және анонимділік жағдайында сәйкестендіру процедураларының дәлдігін арттырады [16].

2.3 Орналастыру үшін Docker пайдалану аналитикалық жүйе

Пайдаланушыны деанонимизациялауға арналған күрделі аналитикалық жүйенің тұрақты және портативті жұмысын қамтамасыз ету үшін Docker контейнерлеу технологиясы қолданылады. Ол барлық тәуелділіктер мен кітапханалар орнатылған оқшауланған орталарға (контейнерлер) бағдарламалық модульдерді бумалауға мүмкіндік береді. Бұл тәсіл жүйені орналастыруды, жаңартуды және масштабтауды айтарлықтай жеңілдетеді [10] [11].

Осы зерттеу аясында жүйенің дамуы деректерді жинау, талдау және визуализациялау модульдерін қамтитын архитектураны құруды қамтыды. Бір конфигурация файлы арқылы бірнеше қатысты контейнерлерді бір уақытта іске қосуға мүмкіндік беретін құрал Docker Compose көмегімен барлық компоненттер бір инфрақұрылымға біріктірілді.

Төмендегі сурет аналитикалық жүйенің сәтті іске қосылғанын растайды:



4-сурет. docker-compose up –d пәрменін пайдаланып контейнерлерді сәтті іске қосу

Суреттен көрініп тұрғандай, жүйе келесі компоненттерден тұрады:

– mongodb – хабарларды, метадеректерді және талдау нәтижелерін сақтайтын дерекқоры бар контейнер.

– enrichment_script_container – деректерді байытуға арналған көмекші модуль (мысалы, уақыт белгілерін, тіл мүмкіндіктерін анықтау).

– telegram-collector – API арқылы Telegram-дан деректерді жинауға арналған модуль.

– қауіп-анализатор – бұл машиналық оқыту үлгілерін қамтитын хабарларды талдау құрамдас бөлігі.

– telegram-notifier – анықталған әрекет туралы хабарламалар жіберетін қызмет.

– бақылау тақтасы – жүйені визуализациялауға және бақылауға арналған веб-интерфейс.

Барлық контейнерлер сәтті жасалды және іске қосылды, бұл дұрыс конфигурацияны және модульдер арасындағы үйлесімділікті көрсетеді. Docker пайдалану мыналарды қамтамасыз етеді:

– икемділік: жүйені Docker қолдауымен кез келген платформада іске қосуға болады;

– ауқымдылық: қажет болған жағдайда жеке модульдерді көшіруге немесе ауыстыруға болады;

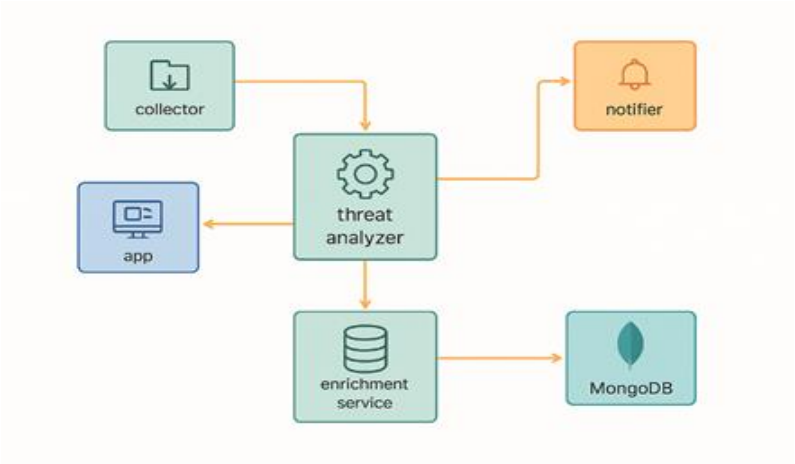
– қайталану мүмкіндігі: тестілеудегі, әзірлеудегі және пайдаланудағы бірдей орта;

– қауіпсіздік: процестерді бір-бірінен және негізгі операциялық жүйеден оқшаулау.

Пайдаланушыны деанонимизациялауға арналған аналитикалық платформа үшін ауқымды және сенімді инфрақұрылымды құру үшін Docker контейнерлеу технологиясы қолданылды. Контейнерлерді пайдалану жүйенің функционалдық модульдерін әрқайсысы қатаң белгіленген тапсырманы орындайтын оқшауланған қызметтерге бөлуге мүмкіндік берді. Бұл тәсіл қайталанымдылықты, орналастырудың қарапайымдылығын және бүкіл жүйені қайта орнатуды қажет етпей-ақ компоненттерді жаңартудың жеңілдігін қамтамасыз етеді [17].

Инфрақұрылым конфигурация файлында көрсетілген барлық модульдерді автоматты түрде іске қосатын Docker Compose көмегімен орналастырылған. Контейнерлер іске қосылған кезде жүйе өз виртуалды желісін жасайды, ол арқылы қызметтер арасында деректер алмасу жүзеге асырылады. Әрбір модульді басқа құрамдас бөліктерден тәуелсіз сынауға немесе масштабтауға болады.

Төмендегі диаграмма аналитикалық жүйенің архитектурасын көрсетеді:



5-сурет. Контейнерленген аналитикалық жүйенің архитектурасы

Компоненттердің сипаттамасы:

– коллектор – API арқылы Telegram-дан хабарламаларды жинауға, әрі қарай талдау үшін деректерді сақтауға арналған модуль;

– қауіп анализаторы – хабарламалардың мазмұнын талдау және анонимді әрекет белгілерін анықтау үшін машиналық оқыту мен NLP үлгілерін пайдаланатын негізгі аналитикалық модуль;

– байыту қызметі – мәліметтерді байытатын көмекші қызмет (мысалы, әрекеттің уақыт аралығын, хабарлама санаттарын және т.б. анықтау);

– MongoDB – хабарлама мәтіндерін, метадеректерді және талдау нәтижелерін сақтайтын дерекқор;

– хабарлаушы – күдікті хабарламалар немесе цифрлық әрекет үлгілері анықталған кезде хабарландыруларды жіберуге жауапты қызмет;

– қолданба (бақылау тақтасы) – деректерді визуализациялауға, сүзгілерді басқаруға және есептерді экспорттауға арналған веб-интерфейс.

Осылайша, Docker деанонимизация жүйесінің инфрақұрылымдық қабаты үшін базалық технология ретінде әрекет етеді. Оны пайдалану тұрақтылықты, тасымалдануды қамтамасыз етеді және нақты зерттеу немесе операциялық ортада енгізуді жылдамдатады.

3 Жүйені практикалық енгізу

Зерттеу аясында жасырын әрекетті және ықтимал күдікті пайдаланушыларды анықтау мақсатында ашық Telegram арналары мен чаттарындағы хабарламаларды автоматтандырылған жинау, өңдеу және талдау үшін аналитикалық жүйе әзірленді және орналастырылды. Жүйе оның икемділігі мен тұрақтылығын қамтамасыз ететін Docker контейнерлеу технологиясын қолданатын модульдік архитектура негізінде жүзеге асырылады.

Хабарламаларды жинау Telegram API интерфейсімен әрекеттесетін телеграмма-коллектор модулі арқылы жүзеге асырылады. Әрбір хабарлама үшін мәтін, күн мен уақыт,

пайдаланушы идентификаторы, пайдаланушы аты (бар болса) және хабардың көзі мен құрылымын көрсететін метадеректер шығарылады. Алынған деректер MongoDB дерекқорында сақталады, ол бөлек контейнерде жұмыс істейді.

Өңдеудің келесі кезеңі мәтінді алдын ала өңдеуді (тазалау, таңбалау, қалыпқа келтіру) және қауіп-анализатор модуліне көшіруді қамтиды, мұнда машиналық оқыту үлгілері пайдаланылады – Random Forest және BERT [18][19]. Бұл алгоритмдер анонимді немесе күдікті әрекетке тән белгілер негізінде хабарламаларды жіктейді, сонымен қатар тілдік және мінез-құлық сипаттамаларын талдайды.

Сонымен қатар, көрсетілген критерийлерге сәйкес келетін хабарламалар анықталса, әкімшілерге немесе жауапты тұлғаларға хабарлама жіберетін жеделхат-хабарлама модулі енгізілді. Бұл ықтимал қауіптерге жауап беру жылдамдығын арттырады [47].

Соңғы компонент бақылау тақтасы болып табылады – талдау нәтижелерін визуализациялауға арналған веб-интерфейс. Ол хабарларды, санаттарды, тәуекел деңгейін және жіберуші мәліметтерін көрсетеді. Бұл зерттеушілерге белсенділік динамикасын қадағалауға, деректерді сүзуге және есептерді экспорттауға мүмкіндік береді.

Жүйе жергілікті және бұлттық орталарда сыналған, нақты уақыт режимінде тұрақты жұмысын көрсетті және цифрлық криминалистикада, әлеуметтік медиа мониторингінде және кибераналитикада пайдалануға бейімделуі мүмкін.

3.1 Telegram API арқылы деректерді жинау және сақтау

Аналитикалық жүйені енгізудің негізгі кезеңдерінің бірі анонимді контент белсенді түрде таратылатын Telegram-дан деректерді автоматтандырылған жинау болып табылады. Telegram қауіпсіз деректер арналарына кедергі жасамай, жалпыға ортақ хабарларға, авторлық ақпаратқа және басқа метадеректерге қол жеткізуге мүмкіндік беретін икемді API ұсынады.

Telegram API [41] қызметіне қол жеткізу үшін my.telegram.org ресми платформасында жеке қосымшаңызды тіркеу қажет. Тіркеу нәтижесінде пайдаланушы Telegram серверіне қосылу кезінде аутентификация үшін пайдаланылатын api_id және api_hash бірегей параметрлерін алады.

Бұл жүйеде қолданылатын конфигурацияның мысалы төмендегі суретте көрсетілген:

6-сурет. Telegram API қолданбасының конфигурациясы (мысал)

Қолданба тіркелгеннен кейін Telethon немесе Pyrogram сияқты клиенттік кітапхана орнатылады. Бұл іске асыруда Telethon Python-дағы ең тұрақты және функционалды түрде кеңейтілген кітапхана ретінде пайдаланылды.

Docker контейнерінде жұмыс істейтін телеграмма-коллектор модулі API арқылы Telegram-ға қосылып, қажетті арналарға, топтарға немесе чаттарға жазылады. Жүйе келесі өрістерді шығарады:

– message_id – хабарламаның бірегей идентификаторы;

– chat_id және chat_title – бастапқы деректер;

– жіберуші_идентификаторы, пайдаланушы аты, телефон_нөмірі – автор идентификаторлары (бар болса);

– message_text – хабарламаның толық мәтіні;

– date_time – уақыт белгісі;

– медиа_түрі, нысандар, жауап беру, қайдан жіберілген – қосымша сипаттамалары контекст .

Telethon көмегімен хабарламаларды алудың мысалы коды:

telethon.sync сайтынан TelegramClient импорттау

клиент = TelegramClient('session_name', api_id, api_hash)

async def collect_messages():

client.iter_messages('target_channel') ішіндегі хабар үшін синхрондау:

басып шығару(хабарлама.sender_id, message.text) [42]

Бұл процесті тізімдер немесе сүзгілер арқылы бірнеше арналар мен чаттарға оңай масштабтауға болады.

Жиналған деректер JSON құжат пішімінде сақтауды қамтамасыз ететін MongoDB дерекқорында сақталады. Әрбір хабарлама кірістірілген құрылымдардан тұратын жеке құжат ретінде сақталады: мәтін, автор, күн, санаттар (егер бар болса), талдау күйі және т.б.

Бұл жағдайда MongoDB артықшылығы оның жартылай құрылымдық мәліметтерді икемді өңдеу мүмкіндігі, сонымен қатар хабарламалар жинағына сұраныстарды өңдеудің жоғары жылдамдығы [43].

MongoDB құжат құрылымының мысалы:

{

«message_id»: 1432,

«text»: «Кіруді қалпына келтіру үшін сілтемені орындаңыз...»,

«username»: «@support_fake_bot»,

«sender_id»: 678901234,

«дата»: «2025-05-15T11:32:00»,

«source»: «@example_channel»,

«risk_score»: нөл,

«is_phishing»: null,

«талданған»: жалған

}

Telegram-да жеке деректер болуы мүмкін болғандықтан, жинақты тек жазылымсыз немесе рұқсатсыз қолжетімді жалпыға қолжетімді хабарламалармен шектеу маңызды. Жүйе рұқсаты шектеулі жеке чаттар, жеке топтар және хабарларды

өңдемейді. Барлық жиналған деректер тек зерттеу мақсатында пайдаланылады және қауіпсіз Docker контейнер ортасында сақталады [20].

Осылайша, Telegram API кеңейтілетін және автоматты хабарламаларды жинауға арналған барлық қажетті құралдарды ұсынады. Алынған деректер цифрлық белсенділікті талдау және деанонимизация жүйесі шеңберінде одан әрі лингвистикалық, мінез-құлық және классификациялық өңдеуге негіз болады.

3.2 Мәтінді алдын ала өңдеу және мүмкіндіктерді шығару

Мәтінді алдын ала өңдеу кез келген мәтіндік ақпаратты талдау жүйесін құрудың міндетті кезеңі болып табылады, әсіресе хабарламаларды жіктеуге және пайдаланушы мінез-құлық сипаттамаларын анықтауға байланысты тапсырмаларда. Бұл кезеңнің мақсаты мәтіндерді талдауға қолайлы форматқа келтіру, сонымен қатар машиналық оқыту алгоритмдерінің жұмысына қажетті негізгі мүмкіндіктерді шығару болып табылады [44].

Бастапқыда Telegram-дан жиналған хабарламалар шулы деректердің үлкен көлемін қамтиды: қосымша бос орындар, арнайы таңбалар, эмодзилер, сілтемелер, пайдаланушы ескертулері және әртүрлі пішімдеу. Бұл элементтер ешқандай пайдалы семантикалық жүктемені көтермейді және талдау нәтижелерін бұрмалауы мүмкін. Сондықтан стандартты алдын ала өңдеу қадамдары қолданылады:

– Мәтінді тазалау: HTML тегтерін, сілтемелерді, арнайы таңбаларды, қайталанатын тыныс белгілерін алып тастаңыз.

– Нормалау: мәтінді кіші әріпке түрлендіру.

– Токенизация: мәтінді жеке сөздерге (лексема) бөлу.

– Тоқтату сөздері: жиі кездесетін, бірақ ақпаратсыз сөздерді алып тастаңыз (мысалы, «бұл», «қалай», «не»).

– Лемматизация: сөздерді негізгі түріне келтіру (мысалы, «төлеу» → «төлеу»).

Мәтіндерді алдын ала өңдеуден кейін мүмкіндіктер шығарылады – машиналық оқыту үлгілері үшін кіріс деректері ретінде пайдаланылатын сандық немесе категориялық сипаттамалар. Ең көп таралған тәсілдер:

– TF-IDF (Term Frequency – Inverse Document Frequency): мәтіндік корпусқа қатысты белгілі бір құжаттағы терминнің маңыздылығын көрсетеді.

– N-граммдар: тұрақты өрнектерді немесе үлгілерді түсіретін N сөздер тізбегі.

– Метафункциялар: хабарламаның ұзақтығы, сілтемелер саны, кілт сөздердің болуы, таңбаларды пайдалану жиілігі, жариялану уақыты мен күні.

Қауіптерді талдау модулінде алдын ала өңдеу және мүмкіндіктерді шығару автоматты түрде орындалады. Нәтижелер әрі қарай мазмұн мен мінез-құлық профилін талдау үшін жіктеу үлгілеріне (Random Forest, BERT) [35] [36] беріледі.

Осылайша, жоғары сапалы алдын ала өңдеу және мәтінді ерекшелендіру деанонимизациялау және пайдаланушы әрекетінің мінез-құлқын бағалау тапсырмаларында сенімді аналитикалық жүйенің негізі болып табылады.

3.3 Хабарлама классификациясы және мінез-құлық талдауы

Мәтінді алдын ала өңдеу және мүмкіндіктерді шығару кезеңінен кейін келесі қадам хабарды жіктеу және пайдаланушы мінез-құлық сипаттамаларын талдау болып табылады. Бұл процестер күдікті әрекет белгілері бар хабарламаларды анықтауға және олардың цифрлық мінез-құлқы негізінде анонимді қатысушылардың профильдерін құруға бағытталған.

Мәтінді классификациялау машиналық оқыту үлгілері арқылы жүзеге асырылады. Бұл жүйе екі үлгіні пайдаланады:

Random Forest – шешім ағаштарына негізделген ансамбльді оқыту алгоритмі. Ол таңбаланған деректер бойынша (санат белгілері бар мәтіндер) оқытылады және жаңа хабарламаның белгілі бір сыныпқа жататын болу ықтималдығын бағалауға мүмкіндік береді (мысалы, күдікті, жалған, зиянсыз).

BERT – сөйлемдегі сөздердің контекстін ескеретін терең нейрондық желі моделі. Бұл әлеуметтік платформаларға тән қысқа, мазмұнды хабарларды талдау үшін әсіресе тиімді. Модель сөз тіркесінің мағынасын түсініп, мәтіннің тональдылығын, мақсатын және тақырыптық фокусын анықтай алады.

Жіктеу процесінде әрбір жаңа хабарлама бұрын оқытылған санаттармен сәйкестіктерге талданады және шекті ықтималдық асып кетсе, оған сәйкес белгі тағайындалады. Нәтижелер мәліметтер базасында сақталады және жүйелік интерфейсте визуализацияланады [31] [32].

Контентті талдаумен қатар қолданушының мінез-құлық талдауы жүргізіледі. Оған мыналар кіреді:

– қызметтің уақытша сипаттамалары (тәулік уақыты, хабарламалардың жиілігі);

– хабарлама құрылымы (ұзындығы, сілтемелердің болуы, эмодзилер, қайталау);

– басқа қатысушылармен өзара әрекеттесу үлгілері (жауаптар, бағыттаушылар);

– басылымдардың ырғағы мен стиліндегі ауытқулар.

Осы деректердің негізінде хабарлар әртүрлі тіркелгілерден жазылған болса да, қайталанатын үлгілер мен күдікті әрекетті анықтауға мүмкіндік беретін мінез-құлық профилі құрастырылады.

Осылайша, жіктеу мен мінез-құлық талдауының үйлесімі деанонимизация жүйесінің мүмкіндіктерін арттырады және нақты хабарламаларды ғана емес, сонымен бірге үйлестірілген немесе зиянды әрекеттерді жүзеге асыратын анонимді қатысушыларды анықтауға мүмкіндік береді [46].

3.4 Пайдаланушыларды деанонимизациялау механизмдері

Пайдаланушылардың деанонимизациясы – цифрлық кеңістікте бүркеншік аттардың, лақап аттардың немесе анонимділіктің техникалық құралдарының артына жасырынған субъектілердің нақты немесе ішінара тұлғасын анықтау процесі. Telegram сияқты әлеуметтік платформалар контекстінде анонимді байланысқа қол жеткізудің жоғары дәрежесіне байланысты деанонимизация әсіресе өзекті болып табылады.

Бұл жүйеде жүзеге асырылатын деанонимизация механизмдері лингвистикалық, мінез-құлық және метадеректер талдауының үйлесімі негізінде жасалған. деректер жинау [33] [34].

1. Метадеректерді салыстыру

Әрбір пайдаланушы үшін хабарлардың техникалық параметрлері жиналады: жариялау уақыты, жіберушінің идентификаторы, пайдаланушы аты (көрсетілген болса), хабарлама тілі, қайта жіберу немесе жауап беру ақпараты. Түрлі чаттардағы мұндай параметрлерді салыстыру әртүрлі тіркелгілердегі қайталанатын мінез-құлық үлгілерін және күдікті әрекетті анықтауға мүмкіндік береді.

2. Лингвистикалық деанонимизация (стилометрия)

Әрбір пайдаланушы ерекше жазу стилімен сипатталады: сөз таңдау, тыныс белгілері, сөйлем құрылымы, эмодзилер мен аббревиатураларды пайдалану. Осы параметрлерді NLP құралдарын пайдаланып талдау арқылы жүйе басқа хабарламалармен салыстыруға болатын тіл профилін жасайды. Осылайша әр түрлі мәтіндердің бір авторға тиесілі екендігі анықталады [45].

3. Мінез-құлық корреляциясы

Пайдаланушы белсенділігі күн уақыты, апта күні, хабар ұзақтығы және тақырып бойынша бақыланады. Жүйе мінез-құлық үлгілерін анықтайды, оларды бір-бірімен салыстырады

және бір пайдаланушының тіркелгілерін біріктіруге мүмкіндік беретін мінез-құлық кластерлерін құрады .

4. Кросс-платформалық OSINT талдауы

Пайдаланушы аты немесе лақап аты ашық көздерде (іздеу жүйелері, басқа әлеуметтік желілер, деректердің ағып кетуі) тексеріледі. Егер атау жеке деректер ашылатын басқа платформаларда пайдаланылса, бұл анонимизацияға қосымша негіз береді.

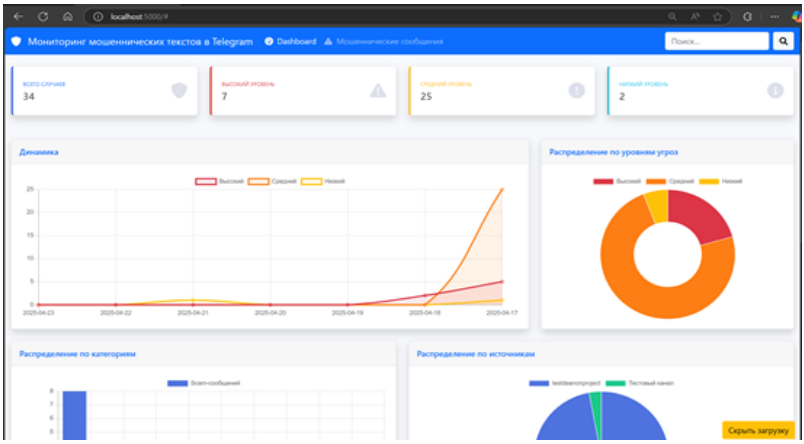
Осылайша, мәтіндерді, мінез-құлықты және ашық деректерді талдауға негізделген деанонимизацияға кешенді көзқарас қатысушыларды олардың жеке басын тікелей ашпаса да анықтауға мүмкіндік береді.

3.5 Веб-интерфейс арқылы нәтижелерді визуализациялау

Нәтижелерді визуализациялау аналитикалық жүйелерде басты рөл атқарады, өйткені ол мәліметтердің үлкен көлемін ыңғайлы түсіндіруді қамтамасыз етеді және пайдаланушыға алынған ақпарат негізінде тез шешім қабылдауға мүмкіндік береді. Бұл жоба ақпаратты графикалық көрсетуге арналған (мысалы, Chart.js, D3.js) Flask құрылымын (немесе FastAPI) және JavaScript кітапханаларын пайдалана отырып әзірленген толық функционалды веб-интерфейсті (Бақылау тақтасы) жүзеге асырды.

Интерфейс жергілікті түрде localhost:5000 сайтында қол жетімді және Telegram-дан алынған хабарламаларды бақылауға және талдауға арналған әкімшілік панель болып табылады. Жүйе графиктер, диаграммалар және кестелер түрінде жинақталған және егжей-тегжейлі деректерді көрсетеді.

Бірінші экранда пайдаланушы жиынтық статистиканы алады: өңделген хабарламалардың жалпы саны, қауіп деңгейі бойынша бөлу (жоғары, орташа, төмен), сондай-ақ алынған оқиғалардың динамикасы.



7-сурет. Аналитикалық жүйенің негізгі панелі

Негізгі көрсеткіштер жоғарғы жағында көрсетіледі:

– Жалпы істер – талданған хабарламалардың жалпы саны;

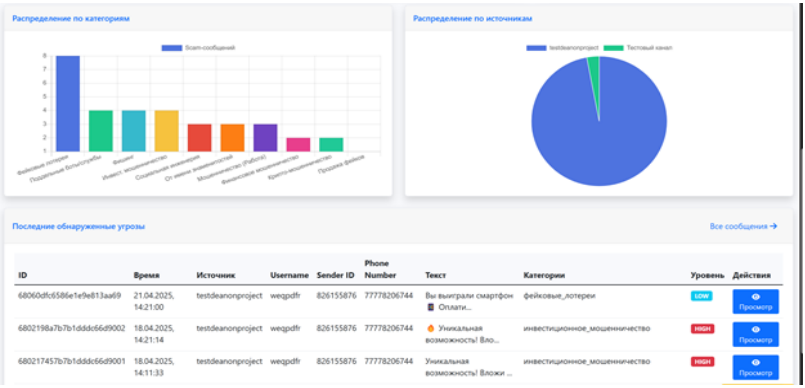
– Жоғары/Орташа/Төмен қауіп – Үлгі бойынша анықталған тәуекелдерді санаттау;

– Динамика графигі – анықталған хабарламалардың өсу уақытының қисығы;

– Сақиналы диаграмма қауіп деңгейлерінің визуалды таралуы болып табылады.

Бұл тәсіл нақты уақытта трендтер мен белсенділік шыңдарын бақылауға мүмкіндік береді.

Панельдегі келесі көрнекі блоктар Санат және Бастапқы диаграммалар болып табылады. Жүйе хабарламаларды алдын ала анықталған түрлерге жіктейді: «инвестициялық алаяқтық», «фишинг», «жалған лотереялар», «әлеуметтік инженерия» және т.б.



8-сурет. Санаттар және Telegram көздері бойынша бөлу

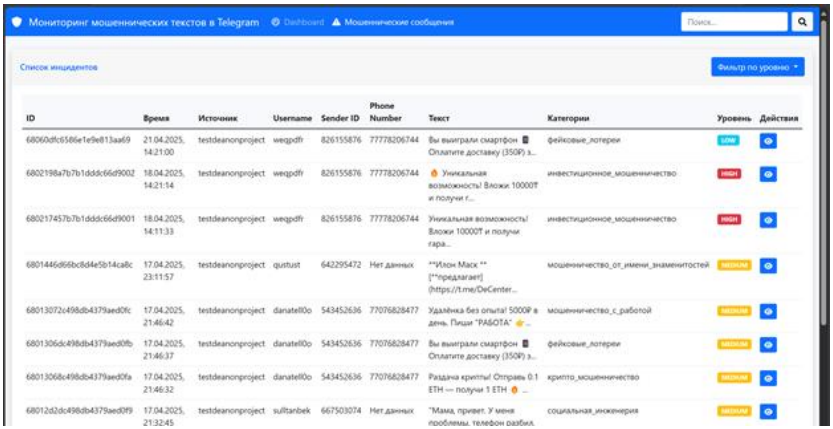
Санат гистограммасы талданатын ағында қандай хабар түрлері басым екенін көрсетеді.

Дөңгелек диаграмма дереккөз бойынша әртүрлі арналар мен чаттардың салыстырмалы үлесін көрсетеді (мысалы, testdeanonproject, сынақ арнасы).

Бұл визуализациялар қызығушылықтың жоғары тәуекел көздерін анықтау және бақылауды шоғырландыру үшін пайдалы.

Төменде әрбір анықталған хабарлама туралы ақпаратты қамтитын кестелер берілген. Пайдаланушы көре алады:

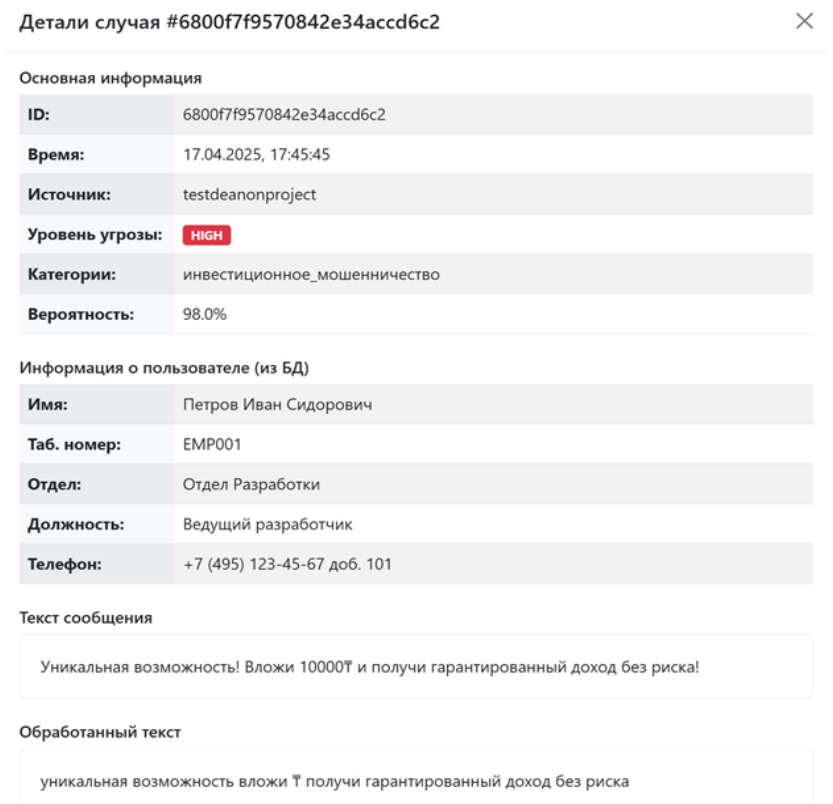
– Қабылдау уақыты;
– Дереккөз атауы (чат, арна);
– Пайдаланушы аты және жіберуші идентификаторы;
– Телефон нөмірі (бар болса);
– Тәуекел категориясы мен деңгейі;
– Мәліметтерді көру функциясы.



9-сурет. Тәуекел деңгейлері бойынша сүзілген анықталған хабарлар кестесі

Сондай-ақ күн, санат, дереккөз немесе қауіп деңгейі бойынша іздеуге және сүзуге болады. Бұл деректермен жұмыс істеу икемділігін қамтамасыз етеді және қызықты жағдайларды жылдам табуға мүмкіндік береді.

«Көру» түймесін басқан кезде істің толық мәліметтері бар модальды терезе ашылады. Негізгі хабарлама деректеріне қосымша дерекқордан болжалды пайдаланушы туралы қосымша ақпарат көрсетіледі (егер оны Жіберуші идентификаторы немесе пайдаланушы аты бойынша сәйкестендіру мүмкін болса).



10-сурет. Оқиға және пайдаланушы туралы толық мәліметтер

Интерфейс мыналарды көрсетеді:

– Хабар идентификаторы және уақыты;

– Қайнар көзі, қауіп деңгейі, категориясы, жіктелу ықтималдығы;

– Пайдаланушы туралы ақпарат (аты-жөні, бөлімі, лауазымы, телефон нөмірі);

– Хабарламаның түпнұсқа мәтіні және оның алдын ала өңделген нұсқасы.

Бұл егжей-тегжейлі деңгей талдаушылар мен қауіпсіздік қызметкерлері үшін хабарларды пайдаланушы дерекқорына сәйкестендіру немесе нақты оқиғаны зерттеу үшін өте маңызды.

Қорытынды

Заманауи цифрлық кеңістік өзара әрекеттесу үшін кең мүмкіндіктер береді, бірақ сонымен бірге ақпараттық қауіпсіздікке әлеуетті қауіп төндіретін анонимді белсенділік деңгейі де артып келеді. Ең аз модерациясы және Telegram сияқты құпиялылығы жоғары платформалар қатысушылардың жеке басын жасыру үшін қолайлы орта жасайды және оқиғаларға жауап беруді қиындатады.

Бұл нұсқаулықтар әлеуметтік орталарда пайдаланушыларды деанонимизациялаудың теориялық және қолданбалы аспектілерін зерттейді. Анонимдік ұғымы талданды, оның негізгі нысандары мен осалдықтары ұсынылды, сандық іздерді талдаудың заманауи әдістері, соның ішінде OSINT құралдары, машиналық оқыту технологиялары және табиғи тілді өңдеу сипатталды.

Контейнерлік технологияларды (Docker) пайдалана отырып, мұндай жүйені енгізу архитектураның ауқымдылығына, сенімділігіне және икемділігіне мүмкіндік береді. Құрылған жүйе Telegram-тағы хабарламаларды талдау мысалы арқылы сыналған және анонимді қатысушыларды анықтау және олардың мінез-құлық профильдерін құрудағы тиімділігін көрсетті.

Ұсынылған материалдар сандық криминалистика, ақпараттық қауіпсіздік және интернет деректерін талдау саласындағы болашақ мамандарды дайындау үшін маңызды. Әдістемелік ұсыныстарды білім беру мақсатында да, әлеуметтік желілердегі белсенділікті талдауға байланысты ғылыми зерттеулер мен қолданбалы жобалар аясында да пайдалануға болады.

Осылайша, әзірленген тәсілдер мен ұсынылған шешімдер қазіргі ақпараттық ортада анонимді қауіптерді анықтау және цифрлық қауіпсіздікті жақсарту бойынша практикалық дағдыларды қалыптастыруға ықпал етеді.

Пайдаланылған әдебиеттер тізімі

1. Vorobyev D., & Kotenko I. (2021). OSINT techniques for social media analysis: A survey. Security and Communication Networks. https://www.hindawi.com/journals/scn/2021/6693845/

2. Wulczyn E., Thain N., & Dixon L. (2017). Ex machina: Personal attacks seen at scale. Proceedings of WWW.

3. Zhong H., Li H., Squicciarini A.C., & Memon N. (2016). Content-driven detection of cyberbullying on the Instagram social network. IJIS.

4. Chen Y., Zhou Y., Zhu S., & Xu H. (2012). Detecting offensive language in social media to protect adolescent online safety. Privacy, Security and Trust Conference.

5. Zhou, Zhiwei, et al. (2021). Hate speech detection on social media: A review. Multimedia Tools and Applications.

6. Zampieri M., et al. (2019). Predicting the type and target of offensive posts in social media. Proceedings of NAACL.

7. Davidson T., Warmsley D., Macy M., & Weber I. (2017). Automated hate speech detection and the problem of offensive language. ICWSM.

8. Basile V., et al. (2019). SemEval-2019 Task 5: Multilingual detection of hate speech against immigrants and women in Twitter. SemEval.

9. Boyd, Danah M., & Ellison, Nicole B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication.

10. Suler J. (2004). The online disinhibition effect. CyberPsychology & Behavior.

11. Brenner, Susan W. (2007). The privacy privilege: The cybersecurity implications of anonymous communication. Journal of Law, Technology & Policy.

12. Balduzzi M., Platzer C., Holz T., Kirda E., & Kruegel C. (2010). Abusing social networks for automated user profiling. RAID.

13. Vorobyev D., & Kotenko I. (2021). OSINT techniques for social media analysis: A survey. Security and Communication Networks.

14. Дьяконов В.А., Ефимова И.В. (2020). Распознавание агрессии и токсичности в социальных сетях с использованием нейросетей. Информационные технологии и телекоммуникации.

15. Карпова О.Н., Петров И.В. (2021). Анализ текстовой агрессии в социальных медиа. Вестник НГУ. Серия: Информационные технологии.

16. Кузнецова Н.В. (2022). Методы и инструменты анализа пользовательской агрессии в интернете. Научно-технические ведомости СПбГПУ.

17. Cheng L., Shu K., Wu S., Silva Y. N., Hall D. L., & Liu H. (2020). Unsupervised Cyberbullying Detection via Time-Informed Gaussian Mixture Model. arXiv preprint arXiv:2008.02642. https://arxiv.org/abs/2008.02642

18. Dadvar M., & Eckert K. (2018). Cyberbullying Detection in Social Networks Using Deep Learning Based Models; A Reproducibility Study. arXiv preprint arXiv:1812.08046. https://arxiv.org/abs/1812.08046

19. Badjatiya P., Gupta S., Gupta M., & Varma V. (2017). Deep Learning for Hate Speech Detection in Tweets. arXiv preprint arXiv:1706.00188. https://arxiv.org/abs/1706.00188

20. Malik J.S., Qiao H., Pang G., & van den Hengel A. (2022). Deep Learning for Hate Speech Detection: A Comparative Study. arXiv preprint arXiv:2202.09517. https://arxiv.org/abs/2202.09517

21. Oakley Browne T., Abedin M., & Chowdhury M.J.M. (2023). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. Artificial Intelligence Review. https://arxiv.org/abs/2202.09517

22. Evangelista J.R.G., et al. (2021). Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. Journal of Applied Security

Research, 16(3), 345-369. https://link.springer.com/chapter/10.1007/978-3-031-45237-6_5

23. Azeez N.A., et al. (2021). Cyberbullying detection in social networks: Artificial intelligence approach. Journal of Cyber Security and Mobility, 10(4), 745-774. https://link.springer.com/chapter/10.1007/978-3-031-45237-6_5

24. Gomez C.E., Sztainberg M.O., & Trana R.E. (2022). Curating cyberbullying datasets: A human-AI collaborative approach. International Journal of Bullying Prevention, 4(1), 35–46. https://link.springer.com/chapter/10.1007/978-3-031-45237-6_5

25. Deliri S., & Albanese M. (2015). Security and privacy issues in social networks. In Data management in pervasive systems (pp. 195–209). Springer. https://link.springer.com/chapter/10.1007/978-3-031-45237-6_5

26. Zhou Z., et al. (2021). Hate speech detection on social media: A review. Multimedia Tools and Applications. https://link.springer.com/article/10.1007/s11042-021-11034-0

27. Basile V., et al. (2019). SemEval-2019 Task 5: Multilingual detection of hate speech against immigrants and women in Twitter. Proceedings of SemEval. https://aclanthology.org/S19-2007/

28. Davidson T., Warmsley D., Macy M., & Weber I. (2017). Automated hate speech detection and the problem of offensive language. ICWSM. https://ojs.aaai.org/index.php/ICWSM/article/view/14955

29. Brenner S.W. (2007). The privacy privilege: The cybersecurity implications of anonymous communication. Journal of Law, Technology & Policy. https://illinoisjltp.com/journal/wp-content/uploads/2013/10/Brenner.pdf

30. Balduzzi M., Platzer C., Holz T., Kirda E., & Kruegel C. (2010). Abusing social networks for automated user profiling. RAID. https://link.springer.com/chapter/10.1007/978-3-642-15512-3_4

31. Aniello Castiglione, Roberto De Prisco, Alfredo De Santis, Ugo Fiore, and Francesco Palmieri. 2014. A botnet-based command and control approach relying on swarm intelligence. Journal of Network and Computer Applications 38 (2014), 22-33.

32. Klingberg S. (2022). Digital Policing of Open Source Intelligence and Social Media Using Artificial Intelligence. In Artificial Intelligence and National Security (pp. 101–111). Springer. https://link.springer.com/chapter/10.1007/978-3-031-06709-9_6

33. Cheng L., et al. (2020). Unsupervised Cyberbullying Detection via Time-Informed Gaussian Mixture Model. arXiv preprint arXiv:2008.02642. https://arxiv.org/abs/2008.02642

34. Dadvar M., & Eckert K. (2018). Cyberbullying Detection in Social Networks Using Deep Learning Based Models; A Reproducibility Study. arXiv preprint arXiv:1812.08046. https://link.springer.com/chapter/10.1007/978-3-031-06709-9_6

35.Badjatiya P., et al. (2017). Deep Learning for Hate Speech Detection in Tweets. arXiv preprint arXiv:1706.00188. https://arxiv.org/abs/2008.02642

36. Malik J.S., et al. (2022). Deep Learning for Hate Speech Detection: A Comparative Study. arXiv preprint arXiv:2202.09517. https://arxiv.org/abs/1812.08046

37. Oakley Browne T., et al. (2023). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. Artificial Intelligence Review. https://arxiv.org/abs/1706.00188

38. Evangelista J.R.G., et al. (2021). Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. Journal of Applied Security Research, 16(3), 345-369. https://arxiv.org/abs/2202.09517

39. Azeez N.A., et al. (2021). Cyberbullying detection in social networks: Artificial intelligence approach. Journal of Cyber Security and Mobility, 10(4), 745-774. https://link.springer.com/article/10.1007/s10207-024-00868-2

40. Gomez C.E., et al. (2022). Curating cyberbullying datasets: A human-AI collaborative approach. International Journal of Bullying Prevention, 4(1), 35-46. https://link.springer.com/chapter/10.1007/978-3-031-45237-6_5

41. Официальный сайт Telegram API: https://core.telegram.org/api

42. Официальная документация Pyrogram: https://docs.pyrogram.org/

43. Vernit Garg and Laxmi Ahuja. 2019. Password Guessing Using Deep Learning. In 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC). IEEE, 38-40.

44. Dongqi Han, Zhiliang Wang, Ying Zhong, Wenqi Chen, Jiahai Yang, Shuqiang Lu, Xingang Shi, and Xia Yin. 2020. Practical traffic-space adversarial attacks on learning-based nidss. arXiv preprint arXiv:2005.07519 (2020).

45. Yisroel Mirsky and Wenke Lee. 2021. The creation and detection of deepfakes: A survey. ACM Computing Surveys (CSUR) 54, 1 (2021), 1-41.

46. Gavai, Gaurang, et al. «Detecting insider threat from enterprise social and online activity data» Proceedings of the 7th ACM CCS international workshop on managing insider security threats. 2015.

47. Zhou, Qingyu, et al. «Neural document summarization by jointly learning to score and select sentences» arXiv preprint arXiv:1807.02305 (2018).

Мазмұны

Беттеу:
Туренова Б.Ю.

Қазақстан Республикасы ІІМ М. Есболатов атындағы
Алматы академиясы ғылыми-зерттеу
және редакциялық-баспа жұмыстарын ұйымдастыру бөлімі
050060, Алматы қ., Өтепов көш., 29

Басуға 02 маусым 2025 ж. жіберілді.
Пішімі 60х84 1/16 №1 баспаханалық қағаз.
Ризографтық басылыс. Есептік баспа табағы 1,3.
Таралымы 50.