https://doi.org/10.58805/itamns.V.1(32)-16

ГИБРИДНАЯ МНОГОУРОВНЕВАЯ СИСТЕМА НА БАЗЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРОТИВОДЕЙСТВИЯ ДЕЗИНФОРМАЦИИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Ұ.М. Өсербеков✉, **А.Т.Тұрарбек**✉

Казахский национальный университет им. аль-Фараби, Алматы, Казахстан
✉ *Корреспондент-автор: oserbekovv@gmail.com, turarbekasem1@gmail.com*

Received: 31 July 2026
Accepted: 10 September 2026
Published: 30 September 2026
Citation: U.M. Osserbekov, et al. « ГИБРИДНАЯ МНОГОУРОВНЕВАЯ СИСТЕМА НА БАЗЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ПРОТИВОДЕЙСТВИЯ ДЕЗИНФОРМАЦИИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ ». Information Technologies, Automation, and Management in Natural Sciences, vol. 1, no. 32, Sept. 2026, doi: https://doi.org/10.58805/itamns.V.1(32)-16
License CC BY 4.0

Во время паводков 2024 года, охвативших несколько областей Казахстана, мессенджеры и социальные сети заполнила волна непроверенных сообщений: ложные сведения о прорывах плотин, завышенные данные о жертвах и откровенные фейки распространялись быстрее официальных сводок и дезорганизовывали работу оперативных штабов. Настоящая работа посвящена разработке системы CrisisStack, способной отличать достоверные сообщения от недостоверных в режиме реального времени. В основе архитектуры - трёхуровневый конвейер: мультиязычный энкодер LaBSE формирует единое векторное представление текста, одномерные свёрточные сети выявляют локальные маркеры манипуляции, двунаправленная LSTM в связке с механизмом самовнимания анализирует контекст сообщения целиком, а мультиагентный протокол сопоставляет предсказание нейросети с данными внешних источников. Обучение проводилось на объединённом корпусе из 35 281 записи открытых наборов WELFake и CrisisMMD с применением смешанной точности. На тестовой выборке из 3 711 записей архитектура достигла Accuracy = 84,9 % и F1 = 0,846, превзойдя базовые модели mBERT (F1 = 0,735) и LaBSE с линейным классификатором (F1 = 0,806).

Исследование методом последовательного исключения показало, что слой внимания вносит наибольший вклад среди компонентов каскада. Перенос модели на казахско-русские тексты без дообучения не достигнут: на открытой выборке аннотированного корпуса zero-shot точность составила 47,3 %, что зафиксировано как ключевое ограничение и определяет направление дальнейшей работы. Протокол верификации проверен в условиях программной имитации внешних источников; время отклика полного конвейера на ускорителе Tesla T4 составило 16,9 ± 1,7 мс.

Ключевые слова: дезинформация, чрезвычайные ситуации, Казахстан, глубокое обучение, LaBSE, механизм внимания, нейросетевая архитектура, мониторинг в реальном времени.

ТӨТЕНШЕ ЖАҒДАЙЛАРДА ДЕЗИНФОРМАЦИЯҒА ҚАРСЫ ТҰРУҒА АРНАЛҒАН ГИБРИДТІ КӨП ҚАБАТТЫ ЖАСАНДЫ ИНТЕЛЛЕКТКЕ НЕГІЗДЕЛГЕН ЖҮЙЕ

Ұ.М. Өсербеков✉, **А.Т.Турарбек**✉

Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
✉ *e-mail: oserbekovv@gmail.com, turarbekasem1@gmail.com*

2024 жылғы Қазақстанның бірнеше облысын қамтыған су тасқыны кезінде мессенджерлер мен әлеуметтік желілерді тексерілмеген хабарламалар толқыны басып қалды: бөгеттердің бұзылуы туралы жалған мәліметтер, құрбандар саны туралы асыра сілтелген деректер және ашық жалған ақпарат ресми хабарламалардан жылдамырақ таралып, жедел штабтардың

жұмысын бұзды. Бұл жұмыс сенімді хабарламаларды сенімсіздерінен нақты уақыт режимінде ажырата алатын CrisisStack жүйесін әзірлеуге арналған. Архитектураның негізі - үш деңгейлі құбыр: көптілді LaBSE энкодері мәтіннің бірыңғай векторлық көрінісін қалыптастырады, бір өлшемді конволюциялық желілер манипуляцияның жергілікті маркерлерін анықтайды, екі бағытты LSTM өзіне назар аудару механизмімен бірге хабарламаның контекстін тұтас талдайды, ал көпагентті хаттама нейрожелінің болжамын сыртқы дереккөздердің деректерімен салыстырады. Оқыту WELFake және CrisisMMD ашық жиынтықтарының 35 281 жазбадан тұратын біріктірілген корпусында аралас дәлдікті қолдана отырып жүргізілді. 3 711 жазбадан тұратын тестілік іріктемеде архитектура Accuracy = 84,9 % және F1 = 0,846 көрсеткіштеріне жетіп, mBERT (F1 = 0,735) және сызықтық жіктеуіші бар LaBSE (F1 = 0,806) базалық модельдерінен асып түсті.

Компоненттерді дәйекті түрде алып тастау әдісімен жүргізілген зерттеу назар аудару қабаты каскад компоненттерінің ішінде ең үлкен үлес қосатынын көрсетті. Модельді қосымша оқытусыз қазақ-орыс тілді мәтіндерге көшіру мүмкін болмады: аннотацияланған корпустың ашық іріктемесінде zero-shot дәлдігі 47,3 % құрады, бұл негізгі шектеу ретінде тіркелді және әрі қарайғы жұмыстың бағытын анықтайды. Верификация хаттамасы сыртқы дереккөздерді бағдарламалық имитациялау жағдайында тексерілді; Tesla T4 үдеткішінде толық жауап беру уақыты 16,9 ± 1,7 мс құрады.

Түйін сөздер: дезинформация, төтенше жағдайлар, Қазақстан, терең оқыту, LaBSE, назар аудару механизмі, нейрондық желі архитектурасы, нақты уақыт режиміндегі мониторинг.

A HYBRID, MULTI-LAYERED AI-POWERED SYSTEM TO COUNTER DISINFORMATION IN EMERGENCY SITUATIONS

U.M. Osserbekov✉, **A.T. Turarbek**✉

Al-Farabi Kazakh National University, Almaty, Kazakhstan
✉*e-mail: oserbekovv@gmail.com, turarbekasem1@gmail.com*

During the 2024 floods that affected several regions of Kazakhstan, messaging platforms and social networks were flooded with unverified reports: false claims about dam breaches, inflated casualty figures and outright fabrications spread faster than official bulletins and disrupted the work of emergency response headquarters. This paper presents CrisisStack, a system designed to separate reliable messages from unreliable ones in real time. The architecture is a three-level pipeline: a multilingual LaBSE encoder produces a unified vector representation of the text, one-dimensional convolutional layers detect local manipulation markers, a bidirectional LSTM combined with self-attention analyses the message context as a whole, and a multi-agent protocol cross-checks the neural prediction against external data sources. The model was trained on a combined corpus of 35,281 records from the open WELFake and CrisisMMD datasets using mixed-precision training. On a held-out test set of 3,711 records the architecture reached an accuracy of 84.9% and a macro-F1 of 0.846, outperforming the mBERT baseline (F1 = 0.735) and LaBSE with a linear classifier (F1 = 0.806).

An ablation study showed that the attention layer contributes the largest single gain among the cascade components. Zero-shot transfer to Kazakh and Russian texts was not achieved: on an open sample of an annotated Kazakh–Russian corpus the model reached 47.3% accuracy, which is reported as a key limitation and defines the direction of future work. The verification protocol was tested under software simulation of external sources; the end-to-end response time on a Tesla T4 GPU was 16.9 ± 1.7 ms.

Keywords: disinformation, emergency situations, Kazakhstan, deep learning, LaBSE, attention mechanism, neural network architecture, real-time monitoring.

Введение. В данное время, когда мир становится все более цифровым, а люди имеют возможность так легко получать новости, очень важно, чтобы информация во время чрезвычайных ситуаций (ЧС) была быстрой и точной. Это напрямую влияет на безопасность страны. Казахстан из-за своего расположения и геологии часто сталкивается с разными природными бедствиями. Например, на севере и западе бывают сильные наводнения, а на юге и юго-востоке часто трясет землю. Как мы увидели весной 2024 года, под водой оказались несколько областей страны, более 100 тысяч человек лишились жилья, и в такие непростые моменты легко распространяются ложные слухи и дезинформация. Эта проблема, которую называют «инфодемией» – когда неправдивая информация бесконтрольно разлетается по мес-

сенджерам вроде Telegram и WhatsApp, а также по соцсетям – очень мешает работе штабов, которые занимаются ликвидацией ЧС, а также органам, сохраняющим порядок и спокойствие общества. Ложные слухи, например, что прорвало плотину, или что стихийные бедствия – дело рук человека, или что гуманитарную помощь раздают неправильно, вызывают панику. Из-за этого люди могут отказываться эвакуироваться, а государственные службы не могут нормально работать. Те системы, которые сейчас используют для отслеживания такой информации, часто работают на ручной проверке или же используют простые фильтры по ключевым словам. Этого достаточно мало, чтобы быстро бороться с угрозами в реальном времени. Автоматически анализировать информацию в Казахстане особенно сложно из-за особенностей языка. В соцсетях люди часто переходят с казахского на русский и обратно, используют сленг, а еще специальные термины, связанные с ЧС. Даже самые продвинутые языковые модели (вроде LLM) не очень хорошо справляются с распознаванием фейков, которые зависят от контекста и характерны именно для Центральной Азии. Им просто не хватает местных данных и глубокой настройки.

Поэтому в этом исследовании мы предлагаем создать особую гибридную систему из нескольких уровней. Она сможет не просто находить дезинформацию, но и помогать активно ей противодействовать. В отличие от того, что есть сейчас, наша система будет объединять глубокие нейросети (например, ансамбль LaBSE-CNN-LSTM) с многоагентным подходом. Это значит, она будет проверять данные по прямым каналам от госорганов, таких как МЧС РК и «Казгидромет». Официальные сводки и показания датчиков используются как опорный источник для сопоставления, с учётом их возможной неполноты и задержки. В этой статье мы хотим рассказать, как мы видим эту многоуровневую систему мониторинга и как ее реализовали. Она должна работать даже при большой нагрузке и быстро реагировать. Дальше мы подробнее рассмотрим, из каких частей состоит система, как обучалась модель и как оценивался её перенос на казахско-русские тексты, а также приведём результаты испытаний протокола верификации в условиях программной симуляции.

Актуальность исследования обусловлена неспособностью существующих систем мониторинга, сфокусированных на ручной модерации или простых фильтрах, по ключевым словам, эффективно выявлять и противодействовать дезинформации в режиме реального времени. Здесь особую сложность представляет лингвистическая специфика Казахстана: активное использование переключения языков (code-switching) между казахским и русским языками, а также использование специфического сленга для данной местности. Поэтому в условиях ЧС стандартные языковые модели без глубокой адаптации демонстрируют низкую точность, что требует создания специализированных гибридных решений, учитывающих региональный контекст и обеспечивающих автоматизированную верификацию данных.

Терминологическое разграничение. В настоящей работе под дезинформацией понимается заведомо ложная информация, распространяемая с намерением ввести в заблуждение; под ошибочной информацией (misinformation) - недостоверные сведения, распространяемые без такого намерения. Термин «фейковая новость» используется как частный случай дезинформации, оформленный в жанре новостного сообщения.

Поскольку намерение автора не может быть установлено автоматически по тексту сообщения, решаемая в работе задача формулируется как бинарная классификация сообщений на достоверные и недостоверные без атрибуции намерения; далее по тексту класс недостоверных сообщений обозначается термином «дезинформация».

Для достижения поставленной цели решались следующие задачи:

1) спроектировать трёхуровневую архитектуру и реализовать её программно (раздел «Материалы и методы», подразделы «Архитектурный дизайн системы» и «Слой L2»);
2) сформировать обучающий корпус и определить протокол разбиения выборок (подразделы «Описание наборов данных» и «Экспериментальный протокол»);
3) экспериментально оценить точность архитектуры в сравнении с базовыми моделями и определить вклад отдельных компонентов (подразделы «Результаты классификации» и «Анализ вклада компонентов»);
4) проверить работоспособность протокола верификации и измерить время отклика системы (подраздел «Верификация данных на основе мультиагентного подхода»).

Целью работы является разработка и программная реализация многоуровневой системы мониторинга CrisisStack, способной идентифицировать дезинформацию в мультиязычных потоках данных и

проводить автоматизированную проверку фактов через интеграцию с внешними, подтвержденными источниками, в том числе государственными органами в условиях высокой информационной нагрузки.

Научная новизна исследования заключается в проектировании гибридной архитектуры, объединяющей три уровня обработки:

- на уровне семантики (L1): Применение мультиязычного инкодера LaBSE, обеспечивающего единое векторное представление для казахских и русских текстов, что создаёт основу для обработки смешанных текстов;
- на уровне классификации (L2): Использование оригинального стека из сверточных (CNN) и рекуррентных (Bi-LSTM) слоев с механизмом Self-Attention, что позволяет одновременно фиксировать триггеры паники и анализировать глубокий контекст сообщения;
- на уровне верификации (L3): Внедрение мультиагентного протокола, который сопоставляет предсказание нейросети с объективными «уликами» из официальных источников (МЧС РК, РГП «Казгидромет»), минимизируя вероятность ложных срабатываний;
- на уровне данных: апробация модели на гибридном корпусе, объединяющем открытые англоязычные наборы WELFake и CrisisMMD, с оценкой кросс-язычного переноса на открытой выборке казахско-русского аннотированного корпуса

В последующих разделах работы подробно рассматривается техническая реализация уровней архитектуры, методология обучения на комбинированных датасетах в среде Google Colab, а также приводятся результаты оценки эффективности модели, включая анализ матрицы ошибок и метрик точности.

Литературный обзор. Исследования в области идентификации дезинформации развиваются по нескольким параллельным направлениям: совершенствование нейросетевых архитектур, разработка систем верификации с привлечением внешних источников и адаптация методов к региональным лингвистическим условиям. Настоящий обзор прослеживает эту эволюцию применительно к задаче детекции дезинформации в условиях чрезвычайных ситуаций.

Первые системы классификации текстов на достоверность опирались на рекуррентные нейронные сети (RNN) [1] и архитектуры долгой краткосрочной памяти (LSTM) [2]. Эти модели впервые позволили учитывать последовательный характер текста, однако плохо справлялись с длинными зависимостями и зашумлёнными данными. Попыткой расширить возможности таких систем стало применение вариационных автокодировщиков для работы с мультимодальным контентом (MVAE) [3], хотя их практическое распространение оказалось ограниченным. Качественный сдвиг в обработке естественного языка обеспечило появление трансформерной архитектуры BERT [4]: модель впервые научилась строить контекстуальные представления слов, учитывая двунаправленный контекст предложения. Это открыло возможность фиксировать тонкие семантические различия между достоверными и манипулятивными текстами. Тем не менее монолитные трансформерные модели имеют принципиальное ограничение: они хорошо улавливают общий смысл, но нередко упускают локальные лингвистические маркеры - агрессивные призывы, характерные для панических фейков конструкции, N-граммы с эмоциональной нагрузкой. Именно это ограничение побудило Keya и соавт. [5] предложить гибридную модель FakeStack, в которой BERT, CNN и LSTM работают совместно: трансформер обеспечивает глубокое семантическое понимание, свёрточные слои выявляют локальные паттерны, а LSTM анализирует глобальную структуру повествования. Альтернативный подход предложен Cui и соавт. [6]: система DETERRENT привлекает графы знаний для верификации утверждений не только на языковом, но и на логическом уровне - проверяя, согласуется ли содержание текста с установленными фактами.

Классификация текста сама по себе не решает проблему дезинформации - она лишь сигнализирует о подозрительном контенте. Для оперативного реагирования необходим следующий шаг: верификация и при необходимости коррекция информации. Gautam [7] формализует этот взгляд в концепции мультиагентных систем (MAS), охватывающих полный жизненный цикл дезинформации: обнаружение, атрибуцию источника и активное опровержение. Качество верификации при этом принципиально зависит от наличия доказательной базы - данного вопроса подробно касается обзор Guo, Schlichtkrull и Vlachos [8], систематизирующий методы автоматической проверки утверждений на основе внешних свидетельств. Отдельную проблему создаёт режим реального времени: в условиях катастрофы каналы связи перегружены, а задержка в несколько секунд может быть критической. Wagner и Roopaei [9] показывают, что перенос части вычислений на периферийные устройства (edge computing) существенно сокраща-

ет время отклика систем экстренного реагирования - подход, который становится особенно актуальным при интеграции ИИ-детекторов в инфраструктуру управления ЧС. Ложные сведения в кризисные периоды несут двойную угрозу: они одновременно разрушают общественное доверие к официальным структурам и дезорганизуют координацию спасательных операций [10]. Это не случайное явление: согласно результатам масштабного исследования Vosoughi, Roy и Aral [11], проведённого на данных Twitter за одиннадцать лет, ложным сообщениям требовалось примерно в шесть раз меньше времени, чем достоверным, чтобы достичь аудитории в 1 500 человек (показатель относится к конкретной методологии авторов и корпусу Twitter). Причём, как показывает Starbird и соавт. [12], за значительной частью дезинформационных кампаний стоит скоординированная активность организованных групп, а не стихийное поведение пользователей. Сочетание высокой скорости распространения с организованным характером кампаний существенно ограничивает возможности мониторинга, опирающегося исключительно на ручную модерацию. ИИ-системы, способные отслеживать динамику информационного поля в реальном времени, открывают качественно новые возможности для государственных структур: Wang и соавт. [13] демонстрируют, как анализ публикаций в социальных медиа позволяет фиксировать фазовые переходы наводнений - нарастание, пик и спад - практически одновременно с физическим развитием события. Теоретические основания для построения подобных систем систематизированы в обзоре Zhou и Zafarani [14], охватывающем фундаментальные методы детекции фейков и актуальные направления их развития. Применение описанных методов к казахстанскому информационному пространству сопряжено с дополнительной сложностью: значительная часть публикаций в социальных медиа не принадлежит ни к чисто казахскому, ни к чисто русскому языку - авторы свободно переключаются между ними в рамках одного сообщения. Долгое время главным барьером для работы с такими текстами оставалось отсутствие специализированных размеченных корпусов. Работа Sambetbayeva и соавт. [15] устранила этот пробел: авторы представили многоуровневую модель аннотирования для детекции фейков на казахско-русском материале с применением платформы Label Studio, сформировав корпус, пригодный для обучения современных нейросетевых моделей. Bolatbek и соавт. [16] применили методы глубокого и машинного обучения к задаче выявления деструктивного контента на казахском языке - подтвердив принципиальную применимость современных NLP-инструментов к этому языку. Тем не менее, при наличии отдельных технологических решений, интегрированная система, объединяющая нейросетевую детекцию дезинформации с реальными оперативными данными государственных ведомств и адаптированная к условиям кризисного управления в Казахстане, до настоящего времени не была предложена. Данный пробел определяет направление настоящего исследования.

Материалы и методы. В данном исследовании предлагается концепция многоуровневой системы верификации контента, которая интегрирует методы глубокого обучения с агентно-ориентированным подходом. В отличие от традиционных детекторов, работающих изолированно, предлагаемая архитектура обеспечивает сквозной цикл: от лингвистического анализа до сопоставления с физическими данными мониторинговых служб.

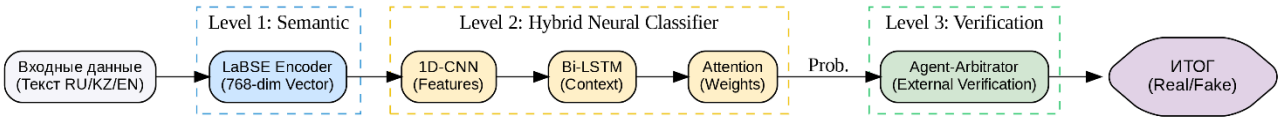


Рис. 1 - Схема архитектуры гибридной системы

Архитектурный дизайн системы. Система реализована в виде последовательного конвейера (Pipeline), разделенного на три иерархических уровня (Рис. 1), что позволяет сочетать глубокое семантическое понимание текста с проверкой фактов в реальном времени:

- L1: Слой семантического выравнивания (Semantic Embedding). На этом этапе входящие сообщения (RU/KZ/EN) трансформируются в единое векторное пространство размерностью 768. Это позволяет системе игнорировать языковой барьер и работать со смыслом сообщения.
- L2: Слой гибридной классификации (Neural Hybrid Stack). Ядро системы, выполняющее многомерный анализ текста с использованием сверточных и рекуррентных нейронных сетей.
- L3: Слой мультиагентной верификации (Verification & Arbitration). Внешний контур без-

опасности, сопоставляющий предсказание нейросети с объективными данными мониторинговых служб (МЧС, Казгидромет).

Слой L2: Гибридная нейросетевая модель.

Центральным элементом классификации является модифицированная архитектура **CrisisStack**. В отличие от стандартных решений, мы реализовали каскадную обработку признаков:

- LaBSE Инкодер: Выполняет роль первичного извлечения признаков. Благодаря обучению на мультиязычных корпусах, энкодер формирует единое представление для казахских и русских текстов; устойчивость к переключению кодов внутри сообщения в настоящей работе отдельно не оценивалась;
- Слой 1D-CNN: Выполняет поиск локальных паттернов (N-грамм). Сверточные фильтры фиксируют маркеры манипуляции, такие как агрессивные призывы к действию или специфические «шумовые» слова;
- Блок Bidirectional LSTM: Отвечает за анализ глобального контекста. Двунаправленность позволяет модели учитывать взаимосвязь между началом и концом сообщения, что критично для выявления логических несоответствий;
- Механизм Self-Attention: Финальный этап нейросетевого анализа. Слой внимания перераспределяет веса токенов, фокусируя модель на наиболее информативных частях текста, определяющих вердикт «фейк».

Выходной слой вычисляет логарифм вероятности принадлежности сообщения к каждому из классов через функцию LogSoftmax:

$$\log P(y = k \mid x) = z_k - \log \sum_{j=1}^{C} \exp(z_j), z = Wc + b \quad (1)$$

где x - входное сообщение; y - метка класса; k ∈ {0, 1} - индекс класса (0 - «достоверно», 1 - «дезинформация»); C = 2 - число классов; c - вектор контекста размерности 256, полученный после слоя Self-Attention; W и b - матрица весов и вектор смещения выходного слоя; z - вектор логитов. Выражение (1) представляет собой стандартную запись функции LogSoftmax; выходная величина является логарифмом вероятности класса и подаётся на функцию потерь NLLLoss.

Слой L3: Агентная логика верификации.

Для снижения риска ошибочных предсказаний высокой уверенности нейросети и минимизации ошибок первого рода (блокировка реальных просьб о помощи) внедрен уровень L3. Практическая реализация включает логику Агента-Арбитра:

- Classifier Agent: Принимает вероятность *P> 0.6* от слоя L2 как сигнал к началу проверки;
- Evidence Retrieval Agent: Инициирует запрос к имитационной базе данных API (например, статус паводков в ЗКО или сейсмоактивности в Алматы);
- Decision Agent (Arbitrator): принимает финальное решение по правилу: если оценка уровня L2 превышает порог и внешний источник не подтверждает аномалию - вердикт «дезинформация»; если оценка превышает порог, но источник подтверждает аномалию (например, критический уровень воды) - автоматический вердикт не выносится и сообщение передаётся оператору с пометкой «требует проверки»; если оценка ниже порога - вердикт «достоверно» с уверенностью, зависящей от согласованности с внешними данными.

Обсуждение и результаты. Целью данного этапа является оценка точности гибридной модели в идентификации дезинформации и проверка работоспособности мультиагентного протокола верификации.

Описание наборов данных и предобработка

Из-за отсутствия, масштабного специализированного датасета по ЧС в открытом доступе для региона Центральной Азии, обучение проводилось в два этапа:

1. Базовое обучение (Pre-training): Использовался корпус WELFake (19 020 записи), что позволило модели изучить общие лингвистические структуры ложных новостей;
2. Доменная адаптация (Fine-tuning): применялся датасет CrisisMMD, содержащий сообщения о реальных природных катастрофах. Для оценки кросс-язычного переноса в тестовую выборку включена открытая выборка казахско-русского корпуса, опубликованного в работе Sambetbayeva и соавт. [15] и размещённого в репозитории github.com/baiangali/fake_news (лицензия CC BY). Выборка содержит 204 записи, после дедупликации - 203. Разметка выполнена авторами корпуса на платформе Label Studio по многоуровневой схеме из девяти категорий; в настоящей работе использована только бинарная разметка

верхнего уровня (FAKE_NEWS / REAL_NEWS), подтипы и семантические отношения не задействованы. Выборка сбалансирована по языкам (100 казахских и 103 русских текста) и по классам внутри каждой языковой группы; медианная длина текста - 37 слов. Данная выборка не пересекается с обучающей частью и использована исключительно для тестирования. Итоговое распределение данных по источникам приведено в таблице 1.

Экспериментальный протокол. Объединённый корпус объёмом 59 684 записи после удаления дубликатов сократился до 35 281 уникальной записи (класс «достоверно» - 19 635, класс «дезинформация» - 15 646). Выборка корпуса [15] была полностью вынесена в тестовую часть до разбиения, что исключает её попадание в обучение. Оставшиеся записи разделены стратифицированно в пропорции 80/10/10: обучающая выборка - 28 065 записей, валидационная - 3 505, тестовая - 3 711 (3 508 внутридоменных записей и 203 записи корпуса [15]). Отсутствие пересечений между выборками контролировалось программно. Дисбаланс классов компенсировался взвешиванием функции потерь: вес класса «достоверно» - 0,8979, класса «дезинформация» - 1,1284.

Таблица 1 - Распределение данных в экспериментальной выборке

Набор данных	**Тип контента**	**Кол-во записей**	**Роль в эксперименте**
WELFake	Общие новости	19 020	Обучение базовым признакам дезинформации
CrisisMMD	Сообщения о ЧС	16 058	Адаптация к терминологии катастроф
Выборка корпуса [15]	KZ/RU новости	203	Zero-shot оценка кросс-язычного переноса
Итого после дедупликации		35 281	Train 28 065 / Val 3 505 / Test 3 711

Таблица 2 - Гиперпараметры обучения

Параметр	**Значение**
Энкодер	setu4993/LaBSE
Максимальная длина последовательности	128 токенов
Физический размер батча	8
Накопление градиентов	4 шага (эффективный батч 32)
Число эпох	8
Скорость обучения, энкодер	5×10^{-6}
Скорость обучения, голова	5×10^{-4}
Оптимизатор	AdamW, weight decay 0,01
Планировщик	OneCycleLR, прогрев 10 %
Обрезка нормы градиента	1,0
Функция потерь	NLLLoss со взвешиванием классов
Смешанная точность	FP16 (torch.amp)
Ранняя остановка	patience = 4
Заморожено слоёв энкодера	4 из 12
Свёрточный слой	768 → 256, ядро 3
Bi-LSTM	2 слоя, скрытое состояние 128
Dropout	0,3

Таблица 3 - Сравнительный анализ точности моделей

Модель / Архитектура	Accuracy	F1-macro
Baseline: Multilingual BERT (энкодер заморожен)	0,7389	0,7352
LaBSE + Dense Layer (энкодер заморожен)	0,8079	0,8060
CrisisStack (LaBSE + CNN + Bi-LSTM + Attention)	0,8488	0,8463

Обучение проводилось в среде Google Colab на графическом ускорителе NVIDIA Tesla T4 (15,6 ГБ видеопамяти, пиковое потребление - 4,53 ГБ). Полное число параметров модели составляет 472 373 635, из них обучаемых 58 740 355 (12,4 %); заморожены эмбеддинги и нижние четыре из двенадцати слоёв энкодера. Гиперпараметры обучения приведены в таблице 2. Для воспроизводимости зафиксировано зерно генератора случайных чисел (seed = 42) и включён детерминированный режим cuDNN.

Результаты классификации (L2 Layer). Анализ эффективности показал, что предложенная гибридная модель LaBSE + CNN + Bi-LSTM + Attention превосходит базовые решения, сопоставление метрик приведено в таблице 3 и на рисунке 4. Внедрение механизма самовнимания (Self-Attention) позволило модели более точно идентифицировать «маркеры паники» (например, призывы к немедленным действиям или неподтвержденные данные о жертвах).

Обучение продолжалось восемь эпох. Наилучшее значение F1-меры на валидационной выборке (0,8713) достигнуто на пятой эпохе; механизм ранней остановки при patience = 4 не сработал, обучение завершилось по исчерпании заданного числа эпох. Динамика функции потерь и метрик приведена на рисунке 2.

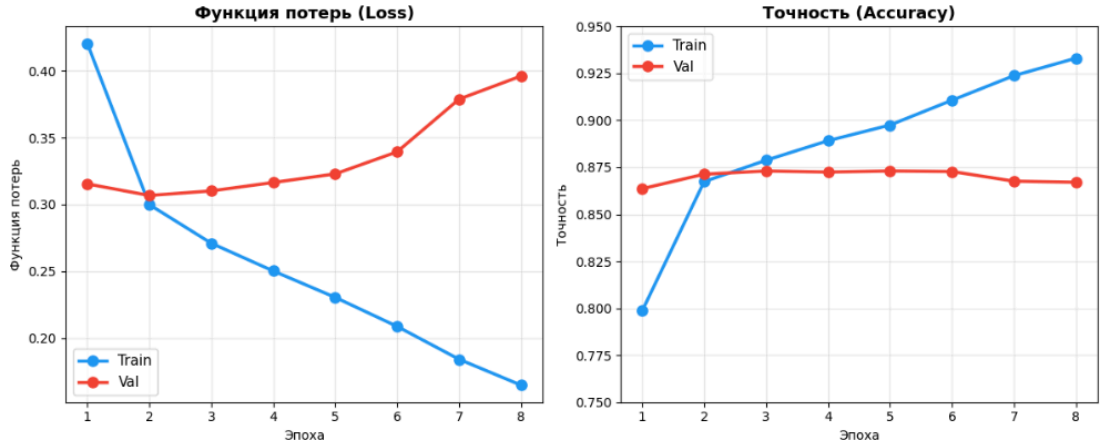


Рис. 2 - Динамика изменения функции потерь (Loss) и точности (Accuracy) в процессе обучения

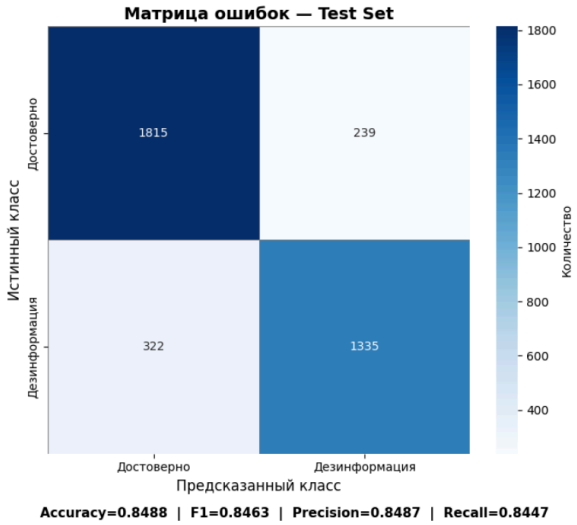


Рис. 3 - Матрица ошибок гибридной модели на тестовой выборке

Анализ графиков (рис. 2) позволяет сделать следующие выводы:

1. График Loss: функция потерь на обучающей выборке монотонно снижается с 0,4207 до 0,1646 за восемь эпох. Потери на валидационной выборке достигают минимума на второй эпохе (0,3068) и далее возрастают до 0,3962, что указывает на переобучение в последних эпохах при сохранении стабильных значений валидационной точности.
2. График Accuracy: точность на валидационной выборке растёт с 0,8636 на первой эпохе до 0,8730 на третьей и далее остаётся в диапазоне 0,8670–0,8730. Итоговая точность на отложенной тестовой выборке (3 711 записей) составила 0,8488 при F1 = 0,8463. Разрыв между валидационной и тестовой метриками объясняется включением в тестовую выборку внедоменной подвыборки корпуса [15].

Для более детального анализа прогностической способности модели была построена матрица ошибок (Confusion Matrix) на тестовой выборке (см. Рисунок 3).

Как видно из рисунка 3, распределение ошибок между классами несимметрично. Полнота на классе «достоверно» составляет 0,8836, тогда как на классе «дезинформация» - 0,8057: система пропускает 19,4 % недостоверных сообщений. Точность по обоим классам практически одинакова (0,8493 и 0,8482), то есть модель не смещена в пользу одного из классов по точности, но менее чувствительна к дезинформации. Ложноположительные срабатывания связаны преимущественно с эмоционально окрашенными достоверными сообщениями, лингвистически схожими с манипулятивными; ложноотрицательные - с фейками, имитирующими нейтральный стиль официальных сводок. Подробные метрики приведены в таблице 4.

Таблица 4 - Метрики по классам на тестовой выборке

Класс	Precision	Recall	F1-score	Записей
Достоверно (0)	0,8493	0,8836	0,8661	2 054
Дезинформация (1)	0,8482	0,8057	0,8264	1 657
Макро-среднее	0,8487	0,8447	0,8463	3 711
Взвешенное среднее	0,8488	0,8488	0,8484	3 711

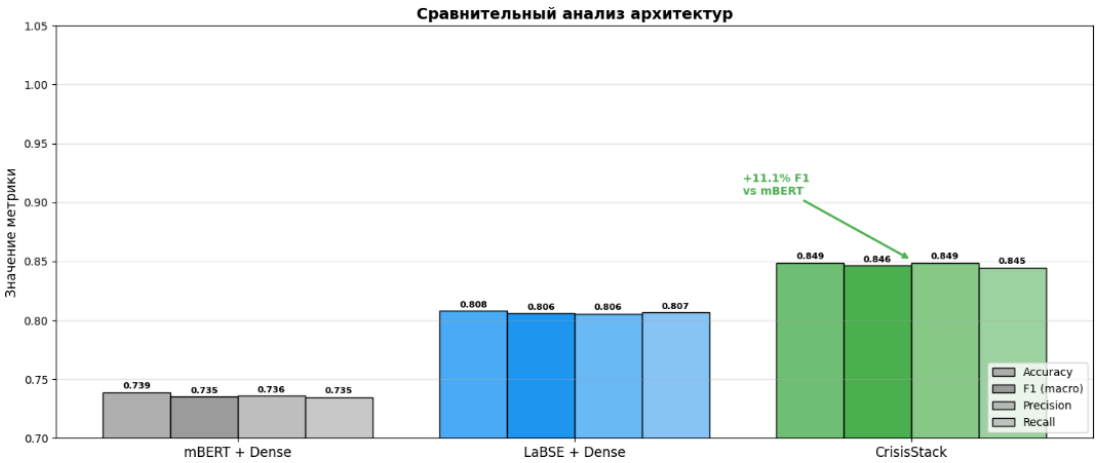


Рис. 4 - Сравнительный анализ архитектур

Анализ вклада компонентов архитектуры. Для количественной оценки вклада отдельных компонентов уровня L2 проведено исследование методом последовательного исключения (ablation study). Все пять конфигураций обучались в идентичных условиях: 11 226 обучающих примеров (40 % выборки, стратифицированный отбор), три эпохи, одно зерно генератора случайных чисел, единый режим оптимизации, совпадающий с описанным в таблице 2. Оценка выполнялась на той же тестовой выборке из 3 711 записей. Результаты приведены в таблице 5.

Полная конфигурация превосходит базовую на 1,67 процентного пункта по F1-мере. Свёрточный и рекуррентный слои по отдельности дают сопоставимый прирост (+0,48 и +0,85 п. п.), однако их совместное применение не аддитивно: конфигурация CNN + Bi-LSTM (0,8337) не превосходит Bi-LSTM в отдельности (0,8344), и различие между ними лежит

в пределах погрешности единичного запуска. Решающий вклад вносит слой внимания, добавляющий 0,88 п. п. поверх связки CNN + Bi-LSTM.

Таблица 5 - Вклад компонентов архитектуры (единый бюджет обучения)

Конфигурация	Accuracy	F1-macro	ΔF1, п.п.
LaBSE + Dense	0,8302	0,8258	-
LaBSE + CNN	0,8340	0,8307	+0,48
LaBSE + Bi-LSTM	0,8378	0,8344	+0,85
LaBSE + CNN + Bi-LSTM	0,8367	0,8337	+0,78
LaBSE + CNN + Bi-LSTM + Attention	0,8453	0,8425	+1,67

Наиболее показательна динамика полноты на классе «дезинформация»: при последовательном добавлении компонентов число пропущенных недостоверных сообщений монотонно снижается с 411 до 336 (полнота растёт с 0,7520 до 0,7972), при этом точность на данном классе остаётся в диапазоне 0,838–0,851. Таким образом, компоненты каскада повышают выявляемость дезинформации, не увеличивая долю ложных срабатываний - размен, существенный для систем мониторинга чрезвычайных ситуаций.

Следует отметить, что базовая конфигурация ablation-эксперимента (0,8258 по F1) превосходит одноимённую строку таблицы 3 (0,8060), поскольку в ablation дообучались верхние восемь слоёв энкодера, тогда как в базовом сравнении энкодер был полностью заморожен. Сопоставление этих величин позволяет разложить итоговый прирост на две составляющие: около 2,0 п. п. обеспечивает дообучение энкодера и около 1,7 п. п. – архитектура каскада CNN + Bi-LSTM + Attention.

Оценка кросс-язычного переноса. Поскольку обучающая выборка сформирована из англоязычных источников (WELFake, CrisisMMD), тестирование на выборке корпуса [15] представляет собой оценку переноса в режиме zero-shot одновременно на казахский и русский языки. Разделение выборки по языку выполнено по наличию девяти специфических букв казахского алфавита; разделение однозначно - в 102 текстах такие символы отсутствуют полностью, в 99 их более десяти, пограничных случаев два. Результаты приведены в таблице 6.

Таблица 6 - Zero-shot оценка по языковым группам

Группа	Записей	Accuracy	F1-macro	Тривиальный базовый уровень
Вся выборка	203	0,4729	0,3576	0,5074
Казахский	100	0,4300	0,3396	0,4900
Русский	103	0,5146	0,3726	0,5243

Перенос обученной модели на казахско-русский домен без дообучения не достигается. Анализ матрицы ошибок показывает, что модель относит к классу «дезинформация» 91 % тестовых сообщений независимо от истинной метки: полнота на классе «достоверно» составляет 0,0588 для казахской части и 0,0408 для русской. Обе величины уступают тривиальному классификатору, всегда предсказывающему класс «дезинформация» (0,4900 и 0,5243 соответственно), поэтому наблюдаемое различие между языковыми группами (+8,46 п. п. по Accuracy в пользу русского) объясняется различием в балансе классов между подгруппами и не свидетельствует о преимуществе переноса на русский язык.

Вероятной причиной является не только языковой, но и семантический сдвиг: в объединённом корпусе класс 1 имеет разное наполнение - в WELFake это заведомо ложные новости, тогда как в CrisisMMD данный класс соответствует признаку «сообщение неинформативно относительно чрезвычайной ситуации». На внутридоменной выборке это различие не препятствует классификации, однако при переносе на короткие политические новости иного домена модель применяет размытый критерий. Унификация семантики меток между источниками рассматривается как первоочередная задача дальнейшей работы.

Верификация данных на основе мультиагентного подхода (L3 Layer). Для оценки функционального уровня L3 проведена программная симуляция обработки пяти сообщений. Ниже подробно разобран один из сценариев - сообщение «В Атырау прорвало трубу водопровода, без воды!», относящееся к пограничной области оценок нейросети:

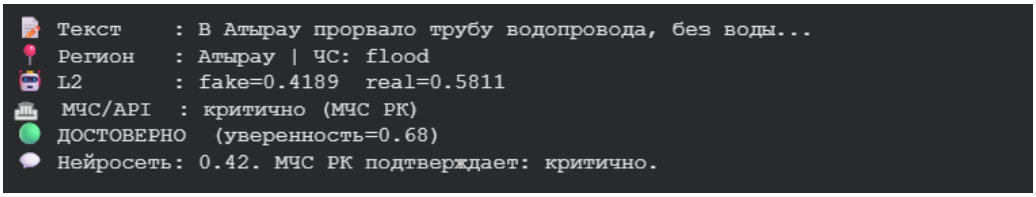


Рис. 5 - Пример интеграции модели с API официальных источников

Цель этапа - проверить, позволяет ли обращение к внешним источникам скорректировать пограничные предсказания нейросети. Тестирование проведено на пяти сценариях, охватывающих паводковую и сейсмическую тематику в четырёх регионах. Процесс верификации включает три этапа, показанные на рисунке 5.

1. Интеллектуальный фильтр (L2). Гибридная модель оценивает вероятность принадлежности сообщения к классу дезинформации. Для приведённого сообщения об аварии водопровода в Атырау получено значение 0,4189, что соответствует пограничной области и не позволяет вынести вердикт исключительно средствами уровня L2.
2. Протокол кросс-верификации (L3). Агент-индексатор определяет географическую привязку (Атырауская область) и тип угрозы (гидрологическая ситуация), после чего выполняет запрос к имитационному API, воспроизводящему структуру ответов РГП «Казгидромет» и оперативных сводок МЧС РК. Запрос возвращает статус «критический уровень воды».
3. Принятие арбитражного решения. Получив подтверждение критической гидрологической обстановки в указанном регионе, агент-арбитр скорректировал вердикт в пользу достоверности сообщения с уверенностью 0,68. Тем самым сообщение о реальной коммунальной аварии в зоне подтверждённого паводка не было заблокировано, несмотря на пограничную оценку нейросети.

По совокупности пяти сценариев система вынесла четыре вердикта «достоверно» и один «требует проверки»; средняя уверенность составила 0,76. Случай «требует проверки» соответствует сценарию, в котором нейросеть оценила сообщение как недостоверное (0,6985), тогда как внешний источник подтвердил критическую обстановку: при таком расхождении протокол не выносит автоматического решения, а передаёт сообщение оператору. Результаты позволяют сформулировать следующие положения. Обращение к внешним источникам данных снижает риск ошибочных предсказаний высокой уверенности в тех случаях, когда официальные сведения по региону доступны. Вместе с тем официальные источники не являются безусловным эталоном: оперативные сводки могут запаздывать относительно развития события или не покрывать локальные инциденты, поэтому расхождение предсказания с внешними данными трактуется протоколом как основание для передачи сообщения оператору, а не как окончательный вердикт. В четырёх из пяти сценариев внешние данные позволили вынести однозначный вердикт при пограничной оценке уровня L2; в одном случае протокол корректно передал сообщение на проверку оператору. Объём выборки сценариев не позволяет делать статистические выводы о частоте ошибок протокола. Время отклика измерено на графическом ускорителе NVIDIA Tesla T4 при длине последовательности 128 токенов: выполнено 10 прогревочных и 100 рабочих прогонов с синхронизацией CUDA. Классификация уровня L2 занимает 16,8 ± 1,6 мс (медиана 16,2 мс, 95-й процентиль 20,7 мс). Полный конвейер с локальным обращением к источнику 16,9 ± 1,7 мс (95-й процентиль 19,7 мс). При моделировании сетевой задержки внешнего API в 200 мс общее время составляет 222,4 ± 4,2 мс (95-й процентиль 230,8 мс). Таким образом, вычислительная составляющая протокола не является узким местом: время отклика определяется преимущественно задержкой обращения к внешнему источнику.

Этические аспекты. Исследование выполнено на публично доступных наборах данных: WELFake и CrisisMMD распространяются для научного использования, выборка корпуса [15] - по лицензии CC BY. Персональные данные авторов сообщений не собирались и не обрабатывались: использовался исключительно текст публикаций без идентификаторов учётных записей, метаданных и сведений о социальных связях. Профилирование пользователей не про-

водилось. Система проектируется как инструмент поддержки принятия решений, а не автоматической модерации. Ошибочная классификация достоверного сообщения о чрезвычайной ситуации как недостоверного способна повлечь непосредственный вред, поэтому архитектура не предусматривает автоматического удаления или блокировки контента: вердикт уровня L3 предназначен для приоритизации сообщений в очереди оператора ситуационного центра. Случаи расхождения нейросетевой оценки с данными внешних источников передаются на рассмотрение человеку. При возможном внедрении системы требуется независимая проверка на предмет систематических смещений в отношении отдельных языковых, региональных и социальных групп.

Ограничения исследования. Полученные результаты следует интерпретировать с учётом следующих ограничений:

1. Уровень L3 проверен в условиях программной имитации. Обращения к API МЧС РК и РГП «Казгидромет» воспроизводились имитационным модулем с фиксированным набором ответов; интеграция с действующими информационными системами ведомств не выполнялась. Приведённые значения уверенности и времени отклика характеризуют логику протокола, но не качество реальных данных и не доступность внешних сервисов.
2. Число сценариев тестирования уровня L3 ограничено пятью. Такой объём достаточен для демонстрации работоспособности логики арбитража, но не позволяет оценить частоту ошибок протокола статистически. + Порог активации проверки (P>0,6) подобран эмпирически по валидационной выборке как компромисс между числом обращений к внешнему источнику и долей пропущенных пограничных случаев. Анализ чувствительности результатов к изменению порога не проводился.
3. Порог активации проверки (P>0,6) подобран эмпирически по валидационной выборке как компромисс между числом обращений к внешнему источнику и долей пропущенных пограничных случаев. Анализ чувствительности результатов к изменению порога не проводился.
4. Перенос на казахско-русский домен без дообучения не достигнут, что подробно рассмотрено в подразделе «Оценка кросс-язычного переноса». Заявленная точность 0,8488 относится исключительно к внутридоменной тестовой выборке.
5. Исследование ablation выполнено при сокращённом бюджете обучения (40 % выборки, три эпохи) и на одном запуске без усреднения по нескольким зёрнам генератора случайных чисел, поэтому различия менее 0,2 п. п. между близкими конфигурациями не следует считать значимыми.
6. Обучающий корпус неоднороден по семантике целевого класса: разметка CrisisMMD отражает информативность сообщения относительно чрезвычайной ситуации, а не его достоверность. Это ограничивает переносимость модели на домены, отличные от обучающего.
7. Устойчивость модели к переключению кодов внутри сообщения, региональному сленгу, опечаткам и сверхкоротким текстам отдельно не проверялась: тестовые данные содержат моноязычные сообщения нормативной орфографии. Оценка устойчивости к этим факторам требует специально сформированного набора и отнесена к дальнейшей работе.

Выводы. Настоящее исследование было мотивировано конкретной практической необходимостью: существующие инструменты мониторинга социальных медиа не справляются с потоком дезинформации в условиях чрезвычайных ситуаций - особенно в информационном пространстве Казахстана, где русский и казахский языки активно смешиваются в одном тексте, а стандартные языковые модели без адаптации дают неудовлетворительные результаты. В ответ на эту проблему была разработана архитектура CrisisStack - трёхуровневая система, в которой глубокое семантическое понимание текста дополнено внешней верификацией через данные государственных органов: эффективность архитектуры подтверждена экспериментально. Последовательная интеграция LaBSE, 1D-CNN, Bi-LSTM и Self-Attention обеспечила Accuracy = 84,9 % и F1 = 0,846, что превышает показатель базовой модели mBERT на +11,1 процентного пункта; вклад компонентов архитектуры определён количественно. Исследование методом последовательного исключения при едином бюджете обучения показало прирост 1,67 процентного пункта по F1-мере для полной конфигурации относительно связки LaBSE + Dense, причём наибольший единичный вклад вносит слой внимания (+0,88 п. п.). Полнота на классе «дезинформация» повышается с 0,7520 до 0,7972 при сохранении точности, то есть каскад увеличивает выявляемость недостоверных сообщений, не повышая долю ложных срабатываний; протокол верификации работоспособен, время отклика измерено. На пяти сценариях получена средняя уверенность 0,76 при четырёх вердиктах «достоверно» и одном «требует проверки». Вычислительная составляющая полного

конвейера составляет 16,9 ± 1,7 мс на ускорителе Tesla T4; при моделировании сетевой задержки внешнего API в 200 мс общее время отклика не превышает 231 мс по 95-му процентилю. Испытания выполнены в условиях программной имитации внешних источников; перенос на казахско-русский домен без дообучения не достигается. Zero-shot оценка дала Accuracy = 0,4729 при F1 = 0,3576; раздельные значения для казахской (0,4300) и русской (0,5146) частей уступают тривиальному классификатору, всегда предсказывающему класс «дезинформация». Установлено, что модель относит к этому классу 91 % внедоменных сообщений независимо от истинной метки. Ограничение носит не только языковой характер: оно связано также с неоднородностью семантики целевого класса в объединённом обучающем корпусе.

Перспективные направления дальнейших исследований определяются выявленными ограничениями и включают: (1) унификацию семантики меток между источниками обучающего корпуса с последующим переобучением; (2) дообучение на казахско-русских данных с применением техник доменной адаптации; (3) расширение исследования ablation до полного бюджета обучения с усреднением по нескольким запускам; (4) анализ чувствительности протокола L3 к выбору порога активации и расширение набора тестовых сценариев; (5) интеграцию с действующими информационными системами МЧС РК и РГП «Казгидромет» с последующей оценкой качества на реальных данных; (6) проверку устойчивости к переключению кодов, сленгу и опечаткам на специально сформированном наборе; (7) интеграцию графовых нейронных сетей для анализа топологии распространения сообщений.

Финансирование. Данное исследование финансировалось Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP26197729).

Литература

1. Ma J., Gao W., Mitra P., Kwon S., Jansen B.J., Wong K.F., Cha M. Detecting rumors from microblogs with recurrent neural networks // The 25th International Joint Conference on Artificial Intelligence (IJCAI 2016). −2016. -P. 3818-3824.
2. Hochreiter S., Schmidhuber J. Long short-term memory // Neural Computation. −1997. -Vol. 9(8). -P. 1735-1780. DOI 10.1162/neco.1997.9.8.1735.
3. Khattar D., Goel P., Gupta M., Varma V. MVAE: Multimodal variational autoencoder for fake news detection // The World Wide Web Conference. −2019. -P. 2915–2921. DOI 10.1145/3308558.3313552.
4. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of deep bidirectional transformers for language understanding // Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics. 2019. -P. 4171-4186. DOI 10.18653/v1/N19-1423.
5. Keya A.J., Shajeeb H.H., Rahman M.S., Mridha M.F. FakeStack: Hierarchical Tri-BERT-CNN- LSTM stacked model for effective fake news detection // PLOS ONE. 2023. -Vol. 18(12): e0294701. DOI10.1371/journal.pone.0294701.
6. Cui L., Seo H., Tabar M., Ma F., Wang S., Lee D. DETERRENT: Knowledge guided graph attention network for detecting healthcare misinformation // Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2020. -P. 492-502. DOI 10.1145/3394486.3403092.
7. Gautam A. Multi-agent systems for misinformation lifecycle: Detection, correction and source identification // arXiv. −2025. -arXiv:2505.17511. DOI:10.48550/arXiv.2505.17511
8. Guo Z., Schlichtkrull M., Vlachos A. A survey on automated fact-checking//Transactions of the Association for Computational Linguistics. - 2022.- Vol. 10.- P.178-206. DOI 10.1162/tacl_a_00454.
9. Wagner J., Roopaei M. Edge based decision making in disaster response systems // 10th Annual Computing and Communication Workshop and Conference (CCWC). −2020. -P. 0469-0473.
10. Komendantova N., Erokhin D. Artificial intelligence tools in misinformation management during natural disasters // Public Organization Review. −2025. -Vol. 25(1). -P. 81-105. DOI 10.1007/s11115-025-00815-2.
11. Vosoughi S., Roy D., Aral S. The spread of true and false news online // Science. −2018. -Vol. 359(6380). -P. 1146–1151. DOI 10.1126/science. aap9559.
12. Starbird K., Arif A., Wilson T. Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations // Proceedings of the ACM on Human-Computer Interaction. 2019. -Vol. 3(CSCW). -P.1-26. DOI 10.1145/3359229.

13. Wang R.Q., Hao H., Yin J., Palen L. Tracking flooding phase transitions and establishing a passive hotline with AI-enabled social media data // IEEE Access. −2020. -Vol. 8. -P. 35515-35525. DOI 10.1109/ACCESS.2020.2994187.
14. Zhou X., Zafarani R. A survey of fake news: Fundamental theories, detection methods, and opportunities // ACM Computing Surveys. −2018. Vol. 53(5):109. DOI 10.48550/arXiv.1812.00315
15. Sambetbayeva M., Nekessova A., Yerimbetova A., Bayangali A., Kaldarova M., Telman D., Smailov N. A multi-level annotation model for fake news detection: Implementing Kazakh- Russian Corpus via Label Studio // Big Data and Cognitive Computing. 2025. -Vol. 9(8): 215. DOI 10.3390/bdcc9080215.
16. Bolatbek M., Sagynay M., Mussiraliyeva Sh., Yeltay Zh. Detection of offensive content in the Kazakh language using machine learning and deep learning approaches // PeerJ Computer Science. 2025. -e3027. DOI 10.7717/peerj-cs.3027.

Информация об авторах

Өсербеков Ұ.М. - магистрант, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан, e-mail: oserbekovv@gmail.com;

Турарбек А.Т. - PhD, и.о. доцента кафедры кибербезопасности и криптологии, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан, e-mail: turarbekasem1@gmail.com.

Information about the authors

Osserbekov U.M. - Master's student, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: oserbekovv@gmail.com;

Turarbek A.T. - PhD, Acting Associate Professor, Department of Cybersecurity and Cryptology, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: turarbekasem1@gmail.com.