Ордена Трудового Красного Знамени Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (МТУСИ)

На правах рукописи

Тетерин Николай Николаевич

Разработка методов и средств интеллектуальной обработки мультимодальных данных из сети Интернет

Специальность 2.3.8 —

«Информатика и информационные процессы»

Диссертация на соискание ученой степени

кандидата технических наук

Научный руководитель:

доктор технических наук, доцент

Саратова Татьяна Евгеньевна

Москва — 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Современное цифровое пространство характеризуется стремительным ростом объемов мультимодального контента. По данным Brand Analytics в марте 2025 года число активных авторов в социальных медиа в России составило 83,8 млн, пользователи написали 1,93 млрд публичных сообщений – постов, репостов и комментариев. По сравнению с мартом 2024 года наблюдается значительный прирост активных пользователей на 22,5% и создаваемого ими контента на 4,3%.

Интернет играет ключевую роль в повседневной жизни, общество все больше зависит от цифровых технологий и интернет-пространства, что приводит к возникновению форм деструктивного поведения пользователей, и становится серьезной проблемой, наносящей вред не только отдельным пользователям, но и целым сообществам и организациям.

Современные технологии, такие как машинное обучение и искусственный интеллект, предоставляют новые возможности для анализа больших объемов данных.

Особенностью предлагаемого исследования является комплексный подход, объединяющий методы машинного обучения и искусственного интеллекта для анализа взаимосвязей между различными типами контента, что не только позволяет выявлять известные формы деструктивного поведения, но и обнаруживать новые, ранее не встречавшиеся паттерны, что особенно важно в условиях быстро меняющегося цифрового пространства.

В условиях усиления деструктивного информационного воздействия как извне, так и внутри страны – интеллектуальная обработка мультимодальных данных из сети Интернет приобретает особую значимость.

Степень разработанности исследования. Существующие работы отечественных исследователей внесли значительный вклад в развитие методов анализа деструктивного контента. Авторы В.В. Тельбух, А.В. Десятых, С.С.

Андрушкевич, Л.П. Пилипенко предложили метод выявления деструктивного контента в интернет-ресурсах на основе комбинированного подхода с использованием Байесовского метода и поиска по словарю.

В.А. Минаев, А.Д. Реброва, А.В. Симонов рассматривали модели классификации текстового контента и методы предварительной обработки для выявления деструктивного поведения в социальных сетях. Авторы исследовали и применяли основные методы векторизации текстов: Bag of Words, TF-IDF, Word2vec.

Роскомнадзор использует автоматизированные системы для мониторинга интернета и выявления запрещенной законом информации, например система «Чистый интернет» состоит из различных модулей, анализирующих текстовую информацию, а система «Окулус» анализирует изображения и видео.

Зарубежные исследователи Z. Ping, Yu. Liu предположили, что мультимодальная интеллектуальная платформа способна эффективно анализировать данные, повышая экономическую выгоду.

Проведенный анализ существующих решений выявил ряд существенных ограничений. Предложенные методы ориентированы на анализ отдельных модальностей и не учитывают взаимосвязи между различными типами данных. Существующие системы преимущественно направлены на выявление уже известных форм деструктивного контента и не обладают достаточной адаптивностью к новым, ранее не встречавшимся паттернам поведения.

Исследование выполнялось в рамках реализации ключевых государственных стратегических документов, направленных на развитие цифровых технологий и обеспечение безопасности, защиту граждан Российской Федерации. Работа соотносится с положениями Национальной стратегии «О развитии искусственного интеллекта на период до 2030 года» (утверждена Указом Президента РФ от 10 октября 2019 г. №490), Национальной стратегии «О комплексной безопасности детей в Российской Федерации на период до 2030 года» (утверждена Указом Президента РФ от 17 мая 2023 г. №358), Национальной стратегии безопасности (утверждена Указом Президента

РФ от 2 июля 2021 г. №400) и относится к национальным интересам Российской Федерации: «сбережение народа России, развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия; укрепление традиционных духовно-нравственных ценностей».

Цель исследования – повышение эффективности и качества выявления деструктивного поведения пользователей в сети Интернет за счет разработки методов и средств интеллектуальной обработки мультимодальных данных.

Объект исследования – цифровой след пользователей в сети Интернет.

Предмет исследования – методы и средства обработки и классификации данных для выявления деструктивного поведения пользователей.

Для достижения поставленной цели были решены следующие **задачи исследования:**

1. Проведен анализ мультимодальных данных и деструктивного поведения в цифровой среде.
2. Разработан метод обработки мультимодальных данных из сети Интернет для интеллектуальных систем.
3. Разработан кросс-модальный вероятностный метод классификации цифровой обработки аудио, текстовых данных, фото и видеоизображений контента.
4. Разработана архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде.
5. Проведен анализ результатов эксперимента.

Методы и методология исследования. В диссертации для решения указанных задач были использованы методы анализа и классификации данных (методы машинного обучения, байесовский анализ), для обработки мультимодальных данных (кросс-модальный анализ, методы предобработки данных), а также для проектирования систем (системный анализ, структурный анализ, объектно-ориентированное моделирование).

Научная новизна.

1. Метод обработки мультимодальных данных из сети Интернет для интеллектуальных систем, *в отличие* от существующих подходов, автоматически формирует новый класс «Z» для потенциально неизвестных случаев деструктивного поведения и реализует интеллектуальную группировку данных по критериям угрозы, что *позволяет* сократить время выявления пользователей, состоящих в деструктивных сообществах в 125 раз, и расширить мультимодальность исследования цифрового следа за счет комплексного анализа данных из сети Интернет (2.3.8, п.7).

2. Кросс-модальный вероятностный метод классификации цифровой обработки аудио, текстовых данных, фото и видеоизображений контента, *в отличие* от существующих методов, реализуется двухэтапная классификация контента за счет оценки вероятности проявления поведения пользователя, *позволяющий* определить принадлежность контента к деструктивному поведению и повысить точность выявления потенциально деструктивного пользователя цифровой платформы на 19% (2.3.8, п.4).

3. Архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде, *в отличие* от известных решений, единый аналитический контур включает сбор данных, специализированные искусственные нейронные сети для каждой модальности данных, кросс-модальную вероятностную классификацию и формирование рекомендаций, что *позволяет* повысить инвариантность к входным показателям без необходимой перенастройки моделей и сократить нагрузку на модераторов интеллектуальной системы (2.3.8, п.16).

Теоретическая и практическая значимость работы определяется установкой критериев интеллектуальной группировки данных по уровням угрозы с учетом мультимодальных признаков, установкой дополнительных признаков классификации со стороны контента и контекста и результатом интеграции разработанных методов и архитектуры является комплексное повышение эффективности и качества выявления деструктивного поведения пользователей в сети Интернет, что проявляется в

оперативности, результативности, ресурсоэкономности, мультимодальности, точности и инвариантности.

Положения, выносимые на защиту:

1. Метод обработки мультимодальных данных из сети Интернет для интеллектуальных систем.
2. Кросс-модальный вероятностный метод классификации цифровой обработки аудио, текстовых данных, фото и видеоизображений контента.
3. Архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде.

Степень достоверности основных полученных результатов обеспечивается надежными исходными данными, адекватностью и корректностью применяемых методов исследования в области искусственного интеллекта и обработки данных. Достоверность подтверждается апробацией и внедрением полученных результатов в практику работы производственных и образовательных организаций.

Апробация работы. Основные положения и результаты диссертационного исследования докладывались и обсуждались на Российских и международных конференциях:

– 2024 4-ая Международная конференция «Technology Enhanced Learning in Higher Education (TELE 2024)» (г. Липецк);

– 2024 Всероссийская научно-практическая конференция «Актуальные проблемы деятельности подразделений УИС» (г. Воронеж);

– 2024 Международная научная конференция «Актуальные проблемы прикладной математики, информатики и механики» (г. Воронеж);

– 2025 Международная научно-практическая конференция «Техника и безопасность объектов УИС» (г. Воронеж).

Личный вклад автора. В ходе исследования автором лично были разработаны и реализованы ключевые подходы, направленные на решение поставленных научных задач. Разработан метод обработки мультимодальных данных из сети Интернет для интеллектуальных систем [82]. Разработан кросс-

модальный вероятностный метод классификации цифровой обработки аудио, текстовых данных, фото и видеоизображений контента [73, 74]. Предложена архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде [72, 75, 83]. Проведен анализ мультимодальных данных и деструктивного поведения в цифровой среде.

Реализация и внедрение результатов исследования. Основные положения диссертационного исследования внедрены в практическую деятельность следующих организаций:

– ООО «НПК «КарбонГрупп» для анализа цифровых взаимодействий сотрудников;

– ООО «АЙТИ КЛАСС» для мониторинга корпоративных коммуникаций сотрудников;

– в учебный процесс Института информационных технологий РТУ МИРЭА.

Подтверждается соответствующими актами внедрения результатов диссертационного исследования, зафиксировавшими значительное повышение качества модерации контента и снижение конфликтных ситуаций.

Соответствие специальности. Тематика и результаты диссертации соответствуют следующим направлениям специальности: 2.3.8 – «Информатика и информационные процессы».

п.7 Разработка методов обработки, группировки и аннотирования информации, в том числе, извлеченной из сети интернет, для систем поддержки принятия решений, интеллектуального поиска, анализа.

п.4 Разработка методов и технологий цифровой обработки аудиовизуальной информации с целью обнаружения закономерностей в данных, включая обработку текстовых и иных изображений, видео контента. Разработка методов и моделей распознавания, понимания и синтеза речи, принципов и методов извлечения требуемой информации из текстов.

п.16 Автоматизированные информационные системы, ресурсы и технологии по областям применения (научные, технические, экономические,

образовательные, гуманитарные сферы деятельности), форматам обрабатываемой, хранимой информации. Системы принятия групповых решений, системы проектирования объектов и процессов, экспертные системы и др.

Публикации. По материалам диссертации опубликовано 17 научных работ (9 статей, 4 материала научных конференций, 4 свидетельства о регистрации программы для ЭВМ), 6 из которых опубликованы в научных журналах и изданиях, рекомендованных ВАК при Министерстве науки и высшего образования Российской Федерации, 1 − в сборнике индексируемом Scopus, в том числе 9 работ опубликованы без соавторов.

Объем и структура работы. Диссертация состоит из введения, 4 глав, заключения, списка литературы и 2 приложения. Полный объем диссертации составляет 133 страницы, включая 48 рисунков и 36 таблиц. Список литературы содержит 131 наименование.

ГЛАВА 1. АНАЛИЗ МУЛЬТИМОДАЛЬНЫХ ДАННЫХ И ДЕСТРУКТИВНОГО ПОВЕДЕНИЯ В ЦИФРОВОЙ СРЕДЕ

Современное цифровое пространство характеризуется стремительным ростом объема и разнообразия пользовательского контента.

Мультимодальные данные представляют собой объединенную разнородную информацию, включающую текстовые сообщения, аудиозаписи, изображения и видеоролики о пользовательской активности. Особенность данных заключается в их взаимодополняющем характере, анализ одного типа контента зачастую дает неполную информацию поведения пользователя. В контексте выявления деструктивного поведения мультимодальность становится важной для выявления угроз в различных форматах.

1.1 Понятие и особенности мультимодальных данных в цифровом пространстве

Мультимодальные данные представляют собой совокупность разнородных цифровых данных, объединяющих различные формы представления информации. В контексте современного интернет-пространства данные формируют основу цифрового следа пользователей и предполагают использование особых подходов к обработке и анализу [6].

Сущность мультимодальности проявляется в одновременном существовании взаимосвязанных, но структурно различных компонентов: текстовые сообщения, аудиоматериалы, визуальный контент [15, 19, 115].

Однако существующие решения, основанные на унимодальных подходах, приводят к высокому проценту ложных срабатываний и возникновению новых угроз.

В таблице 1.1 представлена классификация основных типов мультимодальных данных, используемых при анализе пользовательской активности [1].

Таблица 1.1 – Классификация мультимодальных данных в цифровой среде

Тип данных	**Примеры использования**
Текстовые	Сообщения в чатах, посты в социальных сетях
Аудио	Голосовые сообщения, подкасты
Фото	Фотографии, мемы, скриншоты
Видео	Видеоролики, стримы, видеоконференции

Переходя к анализу структурных особенностей, следует отметить, что мультимодальные данные являются разнородными и включают взаимодействие различных модальностей в цифровом пространстве.

На рисунке 1.1 показано взаимодействие различных модальностей в цифровом пространстве.

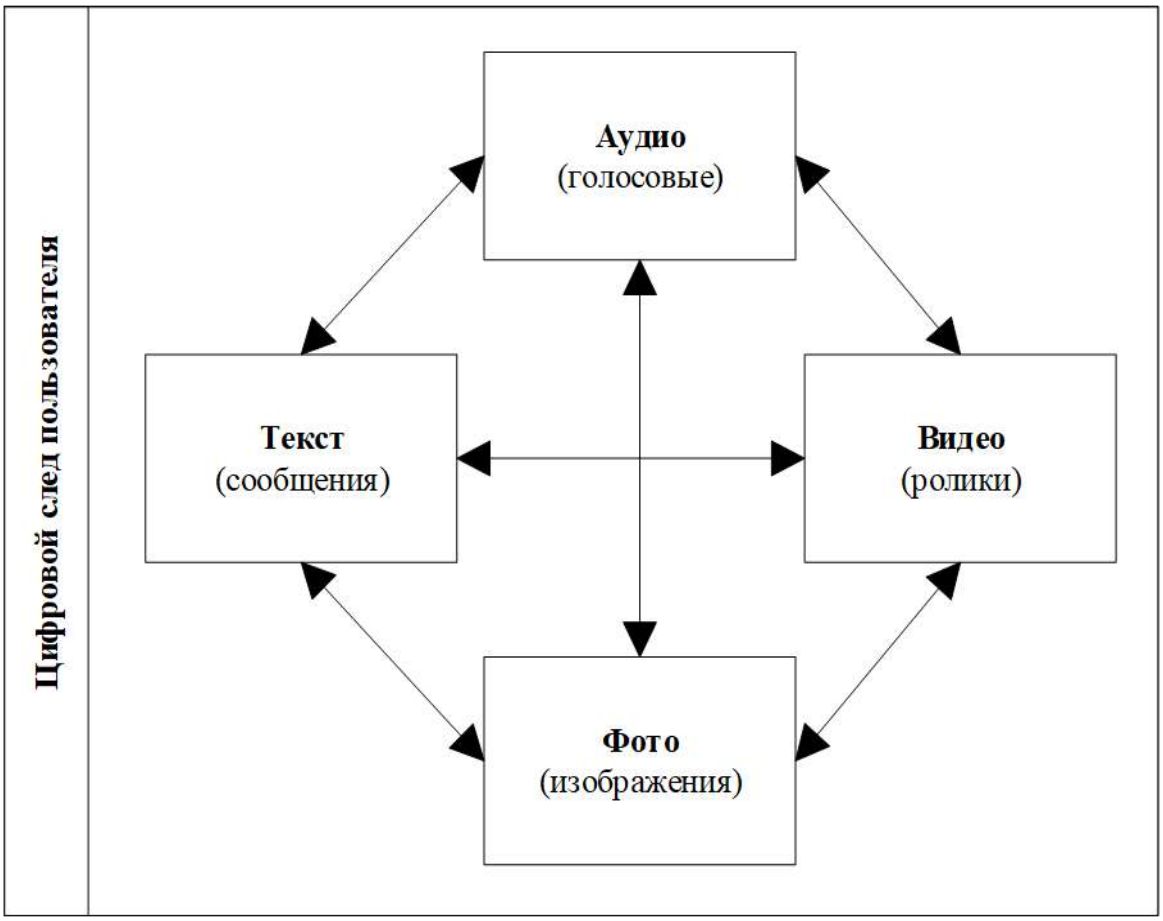


Рисунок 1.1 – Схема взаимосвязи цифровых следов пользователя

На рисунке 1.1 продемонстрировано как различные типы данных взаимосвязаны через общий контекст. Важно отметить взаимодействие модальностей при переходе к анализу деструктивного поведения пользователей, где отдельные модальности могут усилить или ослабить негативный эффект.

Семантическая взаимодополняемость мультимодальных данных проявляется в том, что различные форматы информации содержат взаимодополняющие смысловые компоненты. Например, ирония в текстовом сообщении может подтверждаться определенной интонацией в аудиозаписи, а видео данные способны изменить интерпретацию текстового контента [2].

В таблице 1.2 отображены примеры взаимодействия модальностей с семантической взаимодополняемости.

Таблица 1.2 – Мультимодальные данные на примере семантического взаимодействия

Текст	**Аудио/Видео сопровождение**	**Итоговая интерпретация**
«Отличная работа»	Саркастическая интонация	Критика, недовольство
«Это интересно»	Отсутствие эмоций в голосе, скучающее выражение лица	Скрытое безразличие
Нейтральное описание	Агрессивные жесты на видео	Скрытая угроза

Технологические аспекты обработки мультимодальных данных непосредственно связаны с архитектурой интеллектуальных систем, которая будет подробно рассмотрена в Главе 4. Ключевыми аспектами исследования являются: разработка модулей для каждого типа данных и создание механизмов кросс-модального анализа.

Особую сложность представляет проблема контекстной зависимости, когда идентичные данные в разных ситуациях могут интерпретироваться

противоположным образом. Данный аспект находит свое отражение в кросс-модальном вероятностном методе главы 3.

В образовательной сфере, как в одной из основных областей рассмотрения, мультимодальные данные приобретают особую значимость [9, 10].

Контекстуальная зависимость мультимодальных данных, особенно проявляется при анализе деструктивного поведения. Один и тот же контент в разных ситуациях может содержать скрытую угрозу или быть нейтральным, что подводит к необходимости детального изучения не только технических аспектов обработки данных, но и содержательных характеристик деструктивных проявлений в цифровой среде [129-131].

1.2 Характеристики и виды деструктивного поведения в цифровой среде

Деструктивное поведение в цифровой среде – это поведение, осуществляемое с использованием цифровых технологий и приводящее к нанесению вреда отдельным лицам, группам или обществу в целом [26, 27].

Деструктивное поведение представляет собой поведение, которое приводит к негативным последствиям для самого человека и для общества в целом.

Существует несколько подходов к определению видов деструктивного поведения. Один из них основан на выделении форм поведения, которые наносят вред окружающим людям или самому человеку [24, 25].

К примерам форм деструктивного поведения относят: девиантное поведение, агрессивное поведение, кибербуллинг, троллинг и других форм негативного воздействия.

Девиантное поведение – поведение, которое отклоняется от общепринятых норм и ценностей. Данное поведение может проявляться в различных формах, таких как правонарушения, употребление психоактивных веществ, суицидальное поведение и других форм негативного воздействия.

Агрессивное поведение – поведение, направленное на причинение вреда другому человеку или объекту. Данное поведение может проявляться в физической, вербальной или косвенной форме.

Кибербуллинг – форма травли, которая осуществляется через сеть Интернет или мобильные устройства. Данное поведение может проявляться в виде оскорблений, угроз, распространения ложной информации и других форм негативного воздействия.

Троллинг – форма провокационного поведения, которая направлена на вызов негативных эмоций у других людей. Данное поведение может проявляться в виде оскорблений, провокационных высказываний и других форм негативного воздействия.

Мошенничество – форма деструктивного поведения, заключающаяся в обмане или введения в заблуждения других людей. Данное поведение может проявляться как финансовая махинация, продажа поддельных товаров, предоставление ложной информации и других форм негативного воздействия.

Распространение дезинформации – форма деструктивного поведения, заключающаяся в распространении ложной информации с целью введения в заблуждение других людей. Данное поведение может проявляться с различными целями, такими как получение финансовой выгоды, манипуляция общественным мнением и других форм негативного воздействия.

В таблице 1.3 представлены формы деструктивного поведения и их влияние на организации.

Таблица 1.3 – Влияние форм деструктивного поведения на примере организаций

Форма поведения	**Бизнес-предприятия**	**Образовательные учреждения**
Девиантное поведение	Снижение производительности, ухудшение качества работа	Снижение успеваемости, психологические проблемы

Продолжение таблицы 1.3

Агрессивное поведение	Увеличение вероятности возникновения конфликтов, снижение уровня доверия в коллективе	Увеличение конфликтов, снижение качества образования
Кибербуллинг	Психологическое воздействие на сотрудников, увеличение стресса и депрессии	Психологическое воздействие на студентов и сотрудников
Троллинг	Снижение работоспособности	Снижение эффективности образовательного процесса
Мошенничество	Финансовые потери, ущерб репутации	Финансовые потери, ущерб репутации
Распространение дезинформации	Ухудшение имиджа, потеря доверия	Снижение качества образования, потеря доверия

В представленной таблице видно, что приведенные формы поведения имеют примерно одинаковые серьезные последствия для пользователей и организаций.

Деструктивное поведение может оказывать негативное влияние на взаимодействие между пользователями в контексте структурных подразделений организаций, что приводит к снижению производительности, конфликтным ситуациям между сотрудниками и другим негативным последствиям.

Деструктивное поведение в цифровой среде может быть вызвано различными причинами и факторами, которые можно разделить на несколько категорий.

Факторы и причины возникновения деструктивного поведения в цифровой среде представлены в таблице 1.4.

Таблица 1.4 – Деструктивное поведение в цифровой среде на примере факторов и причин возникновения

Фактор	**Причина возникновения**
Психологический	Низкая самооценка
	Эмоциональная нестабильность
Социальный	Влияние группы
	Социальная изоляция
Культурный	Нормы и ценности
	Медиа и контент
Технологический	Анонимность
	Скорость и доступность информации
Экономический	Финансовые мотивы
	Конкуренция

Применение технологий искусственного интеллекта позволит обрабатывать большие объемы данных и выявлять скрытые закономерности в поведении пользователей. В частности, в Главе 3 будет подробно рассмотрен кросс-модальный вероятностный метод, позволяющий выявлять как явные, так и скрытые формы деструктивного поведения в цифровой среде.

1.3 Обзор современных методов обработки мультимодальных данных

Современные методы обработки мультимодальных данных представляют собой комплексный подход к анализу разнородного цифрового контента. Эффективность выявления деструктивного поведения напрямую зависит от корректности выбора методов.

Методы реализовываются в основных направлениях: текстовые данные, аудио данные и видео данные.

Основу обработки текстовых данных составляют методы обработки естественного языка (Natural Language Processing, NLP). Исторически использовались частотные методы (TF-IDF), однако в настоящее время чаще используют глубокие нейронные сети, позволяющие учитывать семантику и контекст [23].

Основу обработки фотоизображений и видеоданных составляют методы компьютерного зрения (Computer Vision, CV), применяются для классификации изображений, детекции объектов, распознавания сцен и активности [100-104].

Обработка аудиоданных осуществляется в двух основных направлениях: распознавание речи (Automatic Speech Recognition, ASR) для преобразования речевого сигнала в текст с последующим применением NLP-методов и анализ паралингвистических характеристик: тон, тембр, громкость и темп.

Выделяют три основных вида слияния для объединения модальностей.

Раннее слияние (Early Fusion), позднее слияние (Late Fusion) и гибридное слияние (Intermediate Fusion) в таблице 1.5.

Таблица 1.5 – Характеристика и недостатки видов слияния данных

Вид слияния	**Характеристика**	**Недостаток**
Раннее слияние	Предполагает объединение низкоуровневых признаков разных модальностей	Высокая чувствительность к шуму и асинхронности данных
Позднее слияние	Каждая модальность обрабатывается независимой экспертной моделью и объединяются финальные решения	Подход полностью игнорирует межмодальные взаимодействия на промежуточных этапах, теряя семантическую взаимодополняемость
Гибридное слияние	Предполагает создание архитектур, позволяющих моделям для разных модальностей взаимодействовать и обмениваться признаками на различных уровнях	Вычислительная сложность

Несмотря на активное развитие, большинство современных мультимодальных подходов обладают рядом системных ограничений, не

позволяющих эффективно решать задачу выявления деструктивного поведения, которые будут рассмотрены далее.

1.4 Платформы передачи контента и их влияние на анализ мультимодальных данных

Современные цифровые платформы представляют собой уникальную среду для распространения и потребления контента [38-42, 54].

В таблице 1.6 отражены ключевые характеристики основных типов платформ, оказывающих влияние на пользователей и методы анализа мультимодальных данных.

Таблица 1.6 – Сравнительный анализ цифровых платформ по параметрам контента

Параметр	**Социальные сети**	**Мессенджеры**	**Форумы**
Преобладающий тип данных	Текст, изображения, видео	Текст, аудио, изображения, видео	Текст
Уровень модерации	Средний	Низкий	Средний
Скорость распространения	Высокая	Высокая	Низкая

При анализе пользовательской активности в социальных сетях, необходимо учитывать сетевые эффекты и динамику распространения информации. Особую сложность представляет анализ цепочек репостов и комментариев, где контекст может существенно трансформироваться по мере распространения контента.

При анализе пользовательской активности в мессенджерах, необходимо учитывать ограничения по уровням доступа к данным для анализа.

В таблице 1.7 представлена доступность данных для анализа в зависимости от чата.

Таблица 1.7 – Уровни доступа к данным в мессенджерах

Тип коммуникации	Доступные данные	Возможности анализа
Открытые каналы	Полный контент	Мультимодальный анализ
Закрытые группы	Только метаданные	Поведенческие паттерны
Личные сообщения	Нет доступа	Статистические оценки

Форумы представляют собой отдельный класс с преобладанием текстового контента в длинных форматах. Анализ данных требует особых методов обработки естественного языка, способных работать с развернутыми дискуссиями и сложными смысловыми конструкциями

Все вышеописанные особенности цифровых платформ напрямую влияют на разработку методов анализа мультимодальных данных. В главе 4 предлагаемая архитектура системы учитывает данные различия через модульный принцип построения, где каждый компонент может быть адаптирован под конкретный тип платформы.

1.5 Проблемы и вызовы в анализе мультимодальных данных

Проведенный анализ современных методов, платформ и видов деструктивного поведения позволяет выявить ключевые проблемы и вызовы систем автоматической модерации [55-59].

Существующие унимодальные подходы выявления деструктивного поведения представлены далее в исследовании. Для текстовых данных применяются методы векторный (TF-IDF) и семантические (Word2Vec, BERT) для классификации тональности или токсичных высказываний. Для обработки фото и видео изображений используются сверточные нейронные сети (CNN) и детекторы объектов (YOLO), которые обеспечивают распознавание объектов в режиме реального времени. Анализ аудио включает распознавание речи (ASR) с последующим текстовым анализом. Основным недостатком унимодальных

подходов является отсутствие анализа взаимосвязей между модальностями. Систематизация проблем и предлагаемых путей их решения представлена в таблице 1.8.

Таблица 1.8 – Ключевые проблемы и предложения по их решению в рамках исследования

Существующая проблема	**Предложение**
Выявление участников деструктивных сообществ осуществляется ручным анализом огромного объема данных и происходит крайне медленно. Анализ запускается уже после того, как пользователь совершил нарушение.	Повысить **эффективность (Э↑:Оп↑)** выявления пользователей, состоящих в деструктивных сообществах.
На коммуникативных платформах используют унимодальный анализ, что не отражает полной картины поведения пользователя и ведет к грубым ошибкам. Анализ видит только одну сторону контента. Деструктивный контент беспрепятственно проходит модерацию, а безобидный контент, содержащий «опасные» слова в ином контексте – блокируется (ложные срабатывания).	Повысить **качество (К↑:М↑)** исследования цифрового следа за счет комплексного анализа данных из сети Интернет.
Автоматические блокировки за цитирование оскорблений, обсуждение новостей о инцидентах и использование профессионального жаргона. Несправедливые блокировки не отвечают на главный вопрос: является ли пользователь источником деструктивного поведения.	Повысить **эффективность (Э↑:Рез↑)** определения контента деструктивного пользователя.
Высокий процент ложных срабатываний (когда нормального пользователя помечают как угрозу) и ложных пропусков (когда реального нарушителя не находят).	Повысить **качество (К↑:Т↑)** выявления потенциально деструктивного пользователя цифровой платформы.

Продолжение таблицы 1.8

Системы демонстрируют падение точности при изменении характеристик данных, переходе между платформами и появлении новых форматов контента.	Повысить **качество (К↑:ИНС↑)** входных показателей (данные, платформы, области применения) без необходимой перенастройки моделей.
Модераторы перегружены объемом данных и ложными срабатываниями, что приводит к выгоранию и ошибкам.	Повысить **эффективность (Э↑:Ресурс↑)** модераторов интеллектуальной системы.

Данная систематизация проблем и решений определяет критерии оценки разрабатываемых подходов в рамках данного исследования.

1.6 Выводы по главе

В первой главе проведен комплексный анализ существующих методов обработки мультимодальных данных для выявления деструктивного поведения в сети Интернет. Рассмотрены ключевые аспекты мультимодальности, включая особенности взаимодействия текстовых, аудио, фото и видеоданных, а также их семантическую взаимодополняемость. Показано, что мультимодальный подход позволяет более точно интерпретировать поведение пользователей, особенно в контексте скрытых угроз.

Исследованы основные формы деструктивного поведения, а также их влияние на различные сферы, включая бизнес и образование. Выявлены факторы, способствующие возникновению деструктивного поведения: психологические, социальные, технологические и экономические.

Проведен обзор современных методов обработки мультимодальных данных и платформ передачи контента, таких как социальные сети,

мессенджеры и форумы. Установлено, что каждая платформа имеет уникальные характеристики, которые необходимо учитывать при разработке аналитических инструментов.

Основные проблемы, связанные с анализом мультимодальных данных, включают контекстную зависимость, ограниченный доступ к данным в закрытых коммуникациях и сложность обработки разнородных форматов, что требует дальнейшего изучения и разработки адаптивных решений, таких как метод обработки мультимодальных данных и кросс-модальный вероятностный метод, которые будут рассмотрены в последующих главах.

ГЛАВА 2. РАЗРАБОТКА МЕТОДА ОБРАБОТКИ МУЛЬТИМОДАЛЬНЫХ ДАННЫХ ИЗ СЕТИ ИНТЕРНЕТ ДЛЯ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

2.1 Анализ методов обработки мультимодальных данных

Необходимость разработки метода обработки мультимодальных данных обусловлена качественным изменением цифрового контента в сети интернет. Цифровой контент многомерен – текст, аудио, изображения и видео дополняют друг друга, а раздельный анализ данных компонентов дает лишь фрагментарное понимание.

Для комплексного анализа необходимо сначала изучить методы обработки каждого типа данных по отдельности, а затем разработать подход по их объединению. Совместная обработка мультимодальных данных обеспечивает целостное понимание цифрового контента в сети интернет.

2.1.1 Анализ методов обработки текстовых данных

Текстовые данные представляют собой фундаментальный компонент цифрового контента, обладающий уникальными семантическими характеристиками и универсальностью представления информации. Особенности обработки текста обусловлены его дискретностью и сложностью лингвистических взаимосвязей [126].

В разрабатываемом методе для сохранения и формализации семантических, синтаксических и стилистических характеристик текстовых данных в виде математических структур применяется преобразование текста в числовые представления. Данная процедура обусловлена тем, что компьютерные алгоритмы не способны работать с текстом в его естественной форме. Особое значение данный процесс приобретает в мультимодальном подходе, где необходима согласованная обработка разнородных данных.

Преобразование текста в числовые представления осуществляется с использованием следующих ключевых методов:

1. Статистические (TF-IDF);

2. Векторные (Word2Vec);

3. Трансформеры (BERT, GPT, Qwen2.5-7B).

Сравнительная характеристика методов обработки текстовых данных представлена в таблице 2.1.

Таблица 2.1 – Сравнительная характеристика методов обработки текстовых данных

Критерий	**Статистические**	**Векторные**	**Трансформеры**
Учет контекста	Нет	Частичный	Полный
Требования к данным	Высокие	Средние	Низкие
Интерпретируемость	Высокая	Средняя	Низкая
Вычислительная сложность	Низкая	Средняя	Высокая

Для комплексного анализа возможностей трансформерных моделей в задачах обработки текста далее приведены ключевые характеристики BERT, GPT и Qwen2.5-7B в таблице 2.2.

Таблица 2.2 – Сравнение трансформерных моделей

Критерий	**BERT**	**GPT**	**Qwen2.5-7B**
Тип архитектуры	Энкодер	Декодер	Декодер+
Максимальная длина контекста	512 токенов	4К-32К токенов	32К токенов
Поддержка русского языка	Средняя	Хорошая	Оптимизированная
Вычислительные требования	Средние	Высокие	Оптимизированные
Открытость	Полная	Ограниченная	Полная
Лучшее применение	Классификация	Генерация текста	Универсальные задачи

Архитектурные особенности. BERT использует энкодерную архитектуру трансформера, что применимо в задачах классификации и извлечения

сущностей. GPT и Qwen2.5-7B построены на декодерной архитектуре, что делает их более подходящими для генеративных задач. Qwen2.5-7B использует усовершенствованные механизмы внимания и поддерживает обработку сверхдлинных контекстов до 32К токенов.

Таким образом, сравнение демонстрирует, что Qwen2.5-7B в контексте метода обработки мультимодальных данных является универсальной языковой моделью с необходимым в рамках исследования сбалансированным набором характеристик. Qwen2.5-7B в разрабатываемом методе применяет автоматизированное аннотирование для качественной разметки данных.

На начальных этапах для отражения результатов работы метода применялся набор данных, содержащий текстовые сообщения, распределенных по четырем категориям:

1. Сообщения, содержащие запросы информации (вопросы);
2. Сообщения, выражающие недовольство (жалобы);
3. Сообщения с благодарностями или положительными оценками (положительные сообщения);
4. Сообщения, содержащие агрессию или крайний негатив (деструктивное сообщения).

В таблицах 2.3-2.6 показано, что Qwen2.5-7B продемонстрировала высокую точность категоризации.

Таблица 2.3 – Фрагмент набора текстовых данных с категорией сообщения «положительный»

Текст	**Категория**
Преподаватель по математике просто замечательный!	положительный
Спасибо за помощь в оформлении документов!	положительный
Отличная библиотека, всегда нахожу нужные книги!	положительный
Какой прекрасный кампус, здесь так уютно!	положительный

Таблица 2.4 – Фрагмент набора текстовых данных с категорией сообщения «вопрос»

Текст	Категория
Я не могу понять, как подать апелляцию на оценку.	вопрос
Как записаться на дополнительные курсы?	вопрос
Мне нужна помощь с выбором курсов, куда обратиться?	вопрос

Таблица 2.5 – Фрагмент набора текстовых данных с категорией сообщения «жалоба»

Текст	Категория
Этот курс ужасно организован, ничего не понятно!	жалоба
Почему в столовой всегда такие длинные очереди?!	жалоба
Мне не нравится, как проводят лекции, это скучно.	жалоба
Почему никто не отвечает на мои письма?!	жалоба

Таблица 2.6 – Фрагмент набора текстовых данных с категорией сообщения «деструктивный»

Текст	Категория
Зачем вообще нужны эти обязательные предметы?	деструктивный
Я ненавижу этот университет, всё здесь ужасно!	деструктивный
Этот университет — пустая трата времени и денег!	деструктивный

Результаты классификации проанализированы с помощью матрицы ошибок, представленной на рисунке 2.1, которая подтвердила высокую точность модели.

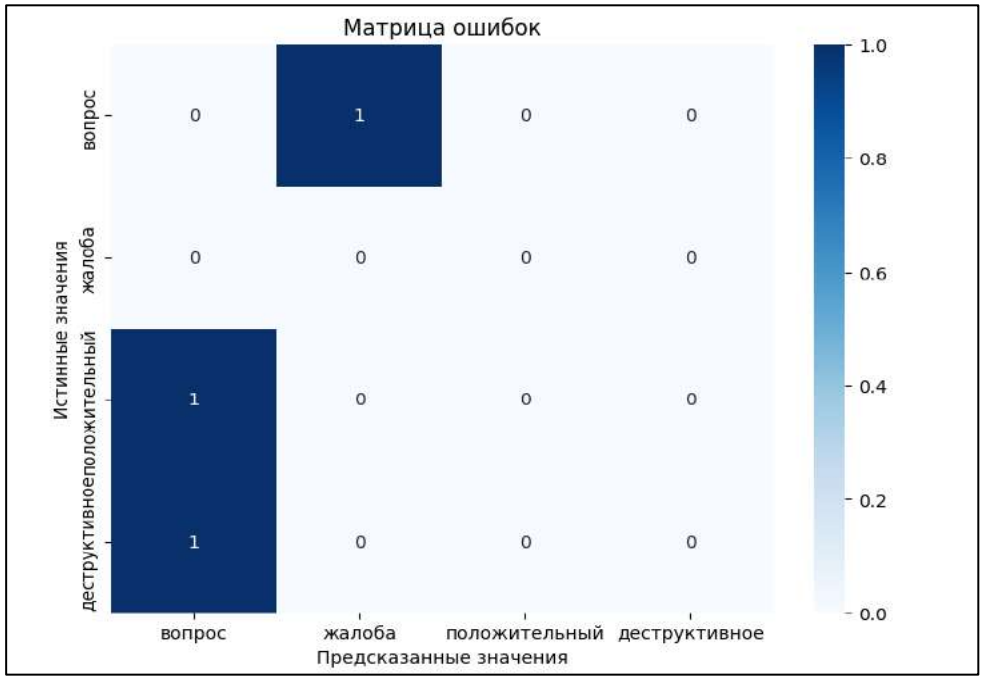


Рисунок 2.1 – Матрица ошибок

Результат анализа значимости признаков, по ключевым словам, для каждой категории продемонстрирован на рисунке 2.2.

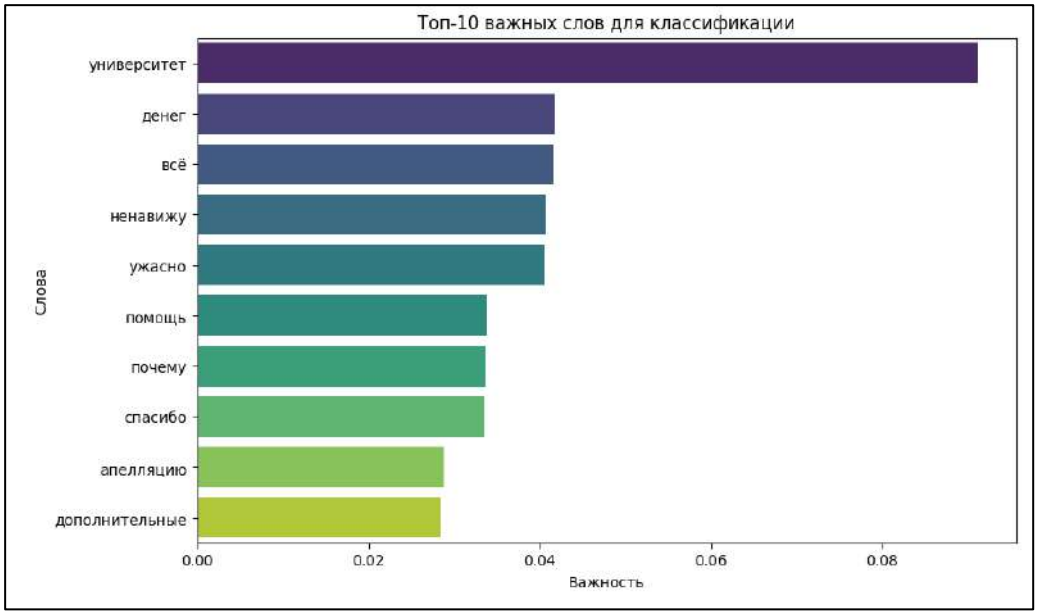


Рисунок 2.2 – Наиболее значимые слова для классификации

Анализ значимости признаков, по ключевым словам, в контексте разрабатываемого метода позволяет:

1. Улучшить интерпретируемость модели для понимания того, какие слова важны, что делает модель более прозрачной и объяснимой.

2. Оптимизировать предобработку данных для выявления значимых слов, что позволяет сосредоточиться на наиболее релевантных признаках и ускорить процесс обработки текста.

3. Повысить точность модели для исключения малозначимых признаков или добавление новых, что повышает качество классификации.

4. Выявить закономерности, для анализа важности слов, помогая понять, какие темы или формулировки чаще всего используются.

Полученные результаты свидетельствуют, что применение автоматизированного аннотирования Qwen2.5-7B создает надежную основу для разрабатываемого подхода.

В контексте разработки метода обработки мультимодальных данных выбор Qwen2.5-7B обусловлен ее способностью глубоко анализировать текстовый контекст и эффективно интегрироваться с другими модулями обработки разнородных данных, например видеоданных.

2.1.2 Анализ методов обработки видеоданных

Современные цифровые пространства, включая социальные сети и корпоративные системы, генерируют огромные объемы видеоконтента, требующего оперативного анализа [105, 109, 111].

Модуль обработки видеоданных в контексте разрабатываемого метода является важным инструментом обеспечения безопасности.

Разрабатываемый подход применим для мониторинга публикаций в социальных сетях и в системах видеонаблюдения, где необходимо оперативно выявлять потенциальные отклонения и угрозы в организационных структурах.

На рисунке 2.3 представлена универсальная схема обработки видеоданных для различных сценариев.

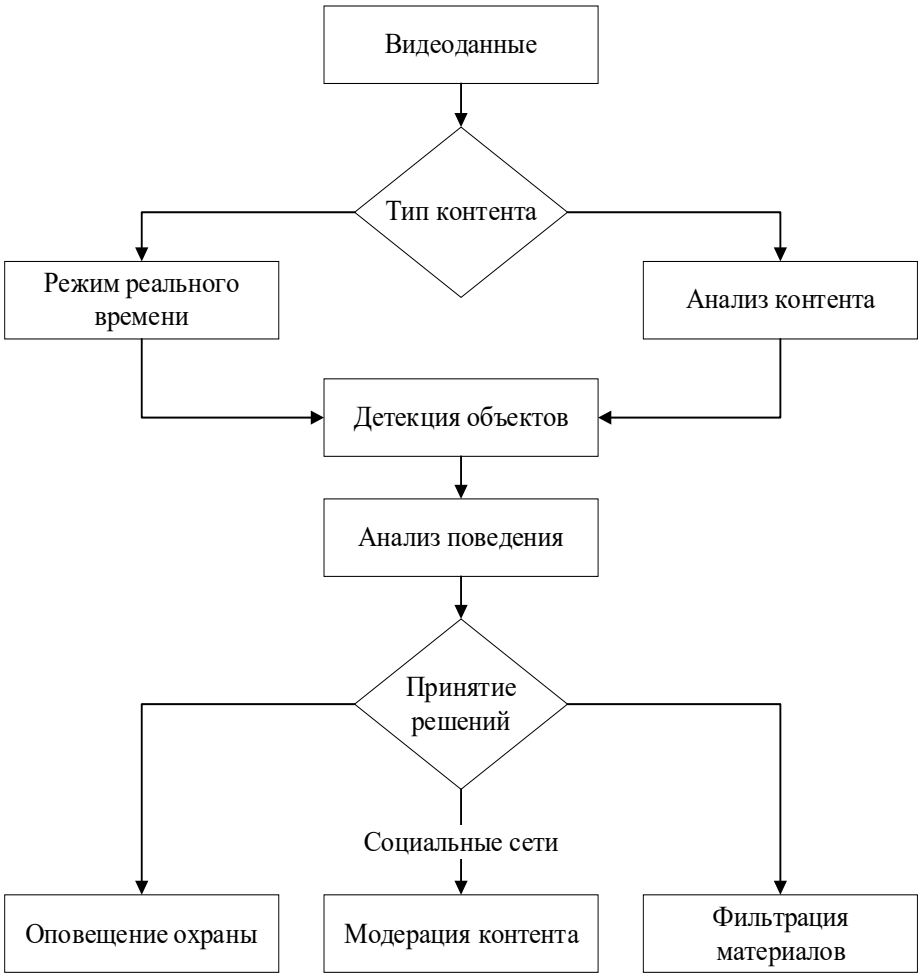


Рисунок 2.3 – Схема обработки видеоданных для различных сценариев

Существующие системы безопасности в организациях, имеют ряд ограничений с точки зрения обработки видеопотоков и детекции:

1. Низкая оперативность реагирования – среднее время обнаружения превышает критический порог для предотвращения отклонения.

2. Субъективность оценки – эффективность обнаружения зависит от внимательности и опыта конкретного сотрудника.

3. Ограниченная масштабируемость – при увеличении количества камер наблюдения пропорционально растет нагрузка на персонал.

Вышеперечисленные факторы обуславливают необходимость видеомониторинга в разрабатываемого метода обработки мультимодальных данных, обеспечивающей: непрерывный анализ видеопотоков в реальном

времени, автоматическое аннотирование инцидентов и мгновенное реагирование на угрозы.

Далее представлен поток обработки видеоданных, в качестве одного из модулей метода, где каждый этап обогащает исходные видеопотоки. Поток обработки данных представлен на рисунке 2.4.

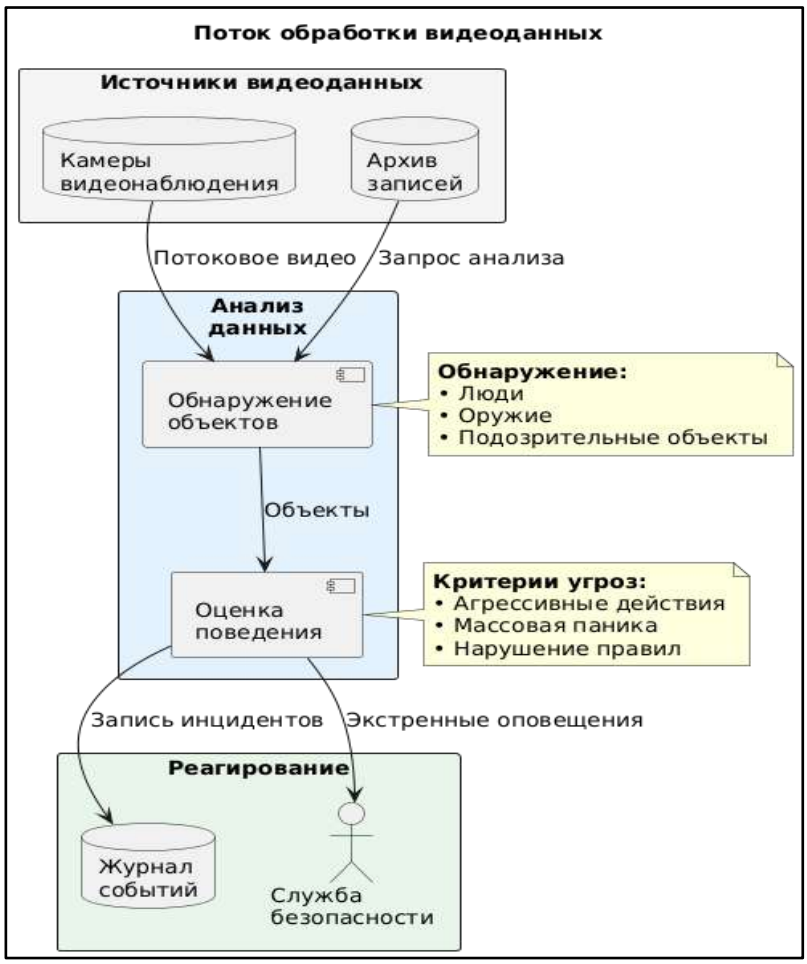


Рисунок 2.4 – Поток обработки видеоданных

Таким образом, встраиваемый в разрабатываемый метод модуль потока обработки видеоданных позволяет решить актуальную проблему обеспечения безопасности в организационных структурах через применение методов обработки видеоданных и автоматического аннотирования инцидентов [113, 114].

Этапы работы модуля обработки видеопотоков с входными и выходными данными представлены в таблице 2.7.

Таблица 2.7 – Этапы работы модуля обработки видеопотоков

Этап	Входные данные	Выходные данные
Детекция объектов	Поток видео с камер Локальные видеофайлы	Координаты местоположения объектов Достоверность обнаружения Тип объекта
Анализ поведения	Координаты местоположения объектов Последовательность кадров	Тип поведения объекта Уровень угрозы Трек ID
Принятие решений	Тип поведения объекта Уровень угрозы Контекст (место, время)	Порядок действия охране Записи в журнал Визуальные метки на видео

На основе анализа существующих решений для обработки видеоданных в рамках разрабатываемого метода сделан выбор в пользу архитектуры YOLO.

Модуль анализа поведений на основе CNN представляет собой глубокую нейросетевую модель, которая анализирует пространственно-временные паттерны в последовательностях видеокадров, используя трехмерные свертки для одновременного учета как пространственных (позы, жесты), так и временных (динамика движений) характеристик поведения.

Модуль детекции объектов на базе YOLO представляет собой высокоэффективную нейросетевую модель для обнаружения людей в видеопотоке, которая анализирует каждый кадр, определяет местоположение и границы всех объектов, при этом адаптивно подстраивая параметры детекции под условия освещенности, плотность людей в кадре и другие факторы, что обеспечивает надежную работу системы в реальном времени при различных сценариях видеонаблюдения [16-18].

В таблице 2.8 представлена сравнительная характеристика методов обработки медиа данных.

Таблица 2.8 – Сравнительная характеристика методов обработки медиа данных

Критерий	**CNN**	**YOLO**
Скорость обработки	Низкая	Высокая
Точность детекции	Средняя	Высокая
Задержка	Высокая	Низкая
Требования к ресурсам	Высокие	Оптимизированные

Данное сравнение демонстрирует, что YOLO в контексте метода обработки мультимодальных данных является универсальной архитектурой с необходимым в рамках исследования сбалансированным набором характеристик. YOLO в разрабатываемом методе применяет автоматизированное аннотирование для качественной разметки данных [118].

В контексте разработки метода обработки мультимодальных данных выбор YOLO обусловлен ее способностью обрабатывать видеопотоки в режиме реального времени, сохраняя высокую точность детекции и эффективно интегрироваться с другими модулями обработки разнородных данных.

2.1.3 Мультимодальные данные

Мультимодальные данные представляют собой комплексную разнородную информацию от текстовых и медиа данных до аудио и метаданных, однако в рамках данного подхода основное внимание уделяется текстовым данным, медиа данным и социальной активности пользователей. Обработка данных включает применение специализированных методов для каждого типа данных с последующим объединением результатов [120-124].

Особенность обработки мультимодальных данных заключается в необходимости объединения разнородных информационных потоков, каждый из которых содержит взаимодополняющие аспекты анализа.

Для текстовых данных применяются методы NLP, включая языковую модель Qwen2.5-7B, которая демонстрирует эффективность в задачах семантического анализа и классификации.

Медиа данные обрабатываются с использованием алгоритмов компьютерного зрения архитектуры YOLOv11, обеспечивающей высокую скорость детекции объектов и анализа поведения в видеопотоках реального времени.

В таблице 2.9 отображены типы данных и их методы обработки.

Таблица 2.9 – Типы данных и их методы обработки

Тип данных	**Методы обработки**	**Ключевые технологии**
Текст	Семантический анализ, классификация	Qwen2.5-7B
Видео и фото	Детекция объектов, анализ поведения	YOLOv11

Объединение модальностей осуществляется через многоэтапный анализ, где каждый модуль отнесен к обработке определенного типа данных, а центральный классификатор демонстрирует результаты для итогового решения.

Мультимодальные данные в контексте разрабатываемого метода объединяют:

1. Текстовые данные;
2. Медиа данные;
3. Социальная активность пользователей.

Таким образом, разработка метода представляет собой комплексный подход.

2.2 Описание этапов метода обработки мультимодальных данных из сети интернет для интеллектуальных систем

Метод представляет собой комплексный подход к анализу пользовательского контента в социальных сетях, объединяющий сбор данных, их модульную обработку и интеллектуальную оценку рисков. В основе подхода лежит синхронизированное применение моделей искусственного интеллекта, каждая из которых относится к анализу определенного типа данных.

Этапы метода обработки мультимодальных данных отображены на рисунке 2.5.

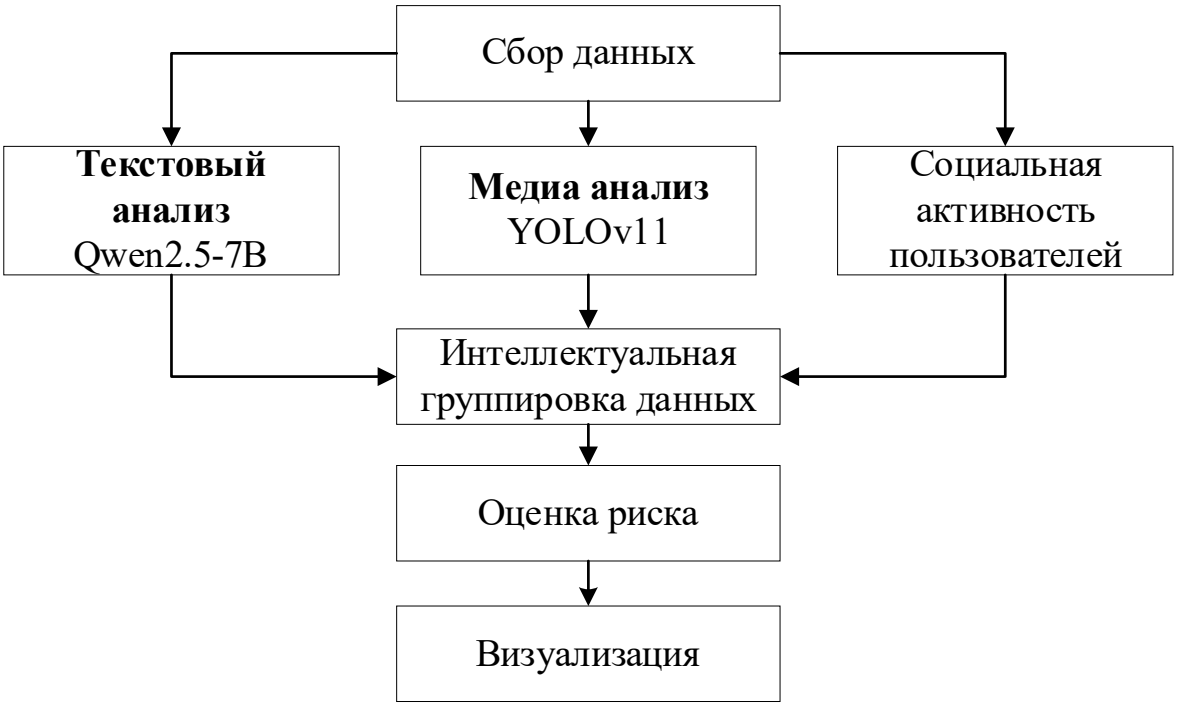


Рисунок 2.5 – Этапы метода обработки мультимодальных данных

На первоначальном этапе осуществляется сбор мультимодального контента, включая текстовые данные, медиа данные и информация о пользователях и их группах. Данные структурируются и подготавливаются для последующего анализа, что обеспечивает их корректную обработку на следующих этапах.

Текстовые данные анализируются языковой моделью Qwen2.5-7B, которая выявляет не только явные признаки, но и скрытые. Медиа контент

обрабатывается моделью компьютерного зрения YOLO для обнаружения объектов и их классификации.

Результаты анализа группируются в единую систему оценки, где пользователи классифицируются по уровню риска: критический, высокий, средний и низкий. Уровень риска определяет значимость каждого из критериев в зависимости от контента.

Схема на рисунке 2.6 демонстрирует объединение данных для комплексной оценки риска.

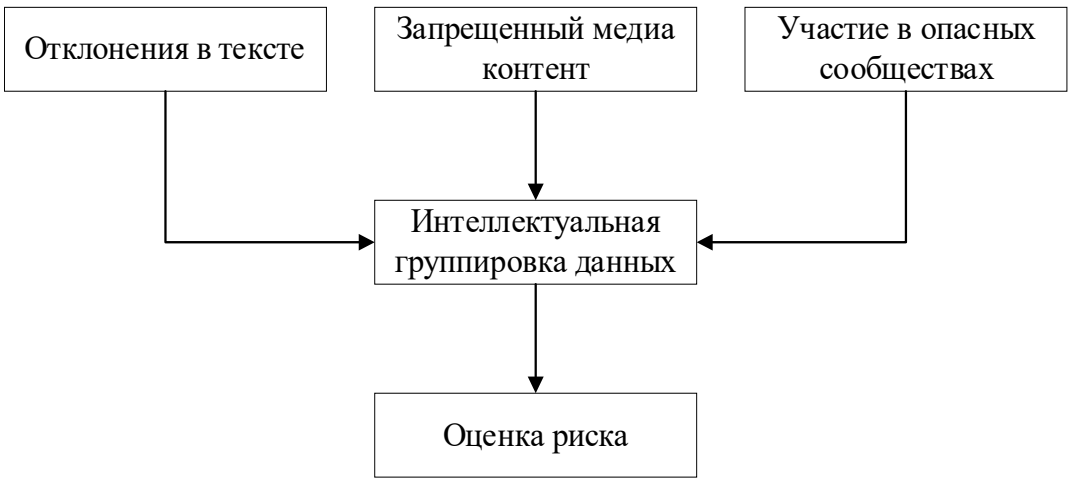


Рисунок 2.6 – Схема процесса интеллектуальной группировки

Обработка данных объединяет 3 модуля, результаты которых группируются по критериям. В рамках данного исследования триггер всех 3 критериев в контексте разрабатываемого метода: деструктивный текст, запрещенный медиа контент и участие в опасных сообществах.

Аналитическое описание метода к процессу присвоения категорий по пользователю на основе анализа его мультимодальных данных по критериям К1, К2 и К3, представлена в формулах 1-8.

Шаг 1. Векторизация и оценка по критериям.

Пусть u – конкретный пользователь. Его цифровой след представлен тремя типами данных:

$D_{text}(u)$ – текстовые данные (посты, комментарии).

$D_{media}(u)$ – медиаданные (изображения, видео).

$D_{social}(u)$ – данные о социальных связях (членство в сообществах).

Для каждого критерия существует специализированная модель, которая преобразует сырые данные в вероятность наличия деструктивных признаков.

1. Критерий К1 (Текстовые данные):

$$f_{К1}: D_{text}(u) \to p_1(u), \quad (1)$$

где $p_1(u) \in [0,1]$ – вероятность того, что текстовый контент пользователя содержит деструктивные элементы.

2. Критерий К2 (Медиаданные):

$$f_{К2}: D_{media}(u) \to p_2(u), \quad (2)$$

где $p_2(u) \in [0,1]$ – вероятность того, что медиаконтент пользователя содержит деструктивные элементы.

3. Критерий К3 (Социальная активность пользователей):

$$f_{К3}: D_{social}(u) \to p_3(u), \quad (3)$$

где $p_3(u) \in [0,1]$ – вероятность того, что пользователь состоит в деструктивных сообществах (нормализованное количество деструктивных сообществ).

В результате для пользователя u формируется вектор риска:

$$p(u) = \big(p_1(u), p_2(u), p_3(u)\big) \quad (4)$$

Шаг 2. Бинаризация оценок по пороговому значению.

Для принятия решения о «совпадении» критерия вводится порог *r*, что позволяет преобразовывать непрерывные вероятности в бинарные решения.

Для каждого критерия $k \in \{1,2,3\}$ определяется бинарная переменная:

$$ck(u) = \begin{cases} 1, \text{если } pk(u) \geq r \text{ (критерий совпал, риск обнаружен)} \\ 0, \text{если } pk(u) < r \text{ (критерий не совпал, риск не обнаружен)} \end{cases} \quad (5)$$

Таким образом, пользователь *u* описывается бинарным вектором совпадений:

$$\mathrm{c}(u) = \big(\mathrm{c}_1(u), \mathrm{c}(u), \mathrm{c}_3(u)\big) \quad (6)$$

Шаг 3. Правило интеллектуальной группировки (присвоение категории риска).

Категория риска *R(u)* присваивается пользователю u на основе нормы (длины) его бинарного вектора совпадений *c(u)*. Норма $L1$ вектора (вес Хемминга для бинарных векторов) равна количеству единиц в нем:

$$||\mathrm{c}(u)||_1 = \mathrm{c}_1(u) + \mathrm{c}(u) + \mathrm{c}_3(u) \quad (7)$$

Правило группировки, представленное в таблице 5:

$$R(u) = \begin{cases} \text{Критический, если } ||\mathrm{c}(u)||_1 = 3 \\ \text{Высокий, если } ||\mathrm{c}(u)||_1 = 2 \\ \text{Средний, если } ||\mathrm{c}(u)||_1 = 1 \\ \text{Низкий, если } ||\mathrm{c}(u)||_1 = 0 \end{cases} \quad (8)$$

В таблице 2.10 приведены категории риска и их критерии на основе интеллектуальной группировки.

Таблица 2.10 – Критерии интеллектуальной группировки для оценки риска

Категория риска	**Критерии**
Критический	Совпадение по всем 3 критериям
Высокий	Совпадение по 2 любым критериям из 3
Средний	Совпадение по 1 критерию из 3
Низкий	Отсутствие совпадений по критериям

Логическая диаграмма на рисунке 2.7 демонстрирует объединение критериев для комплексной оценки риска.

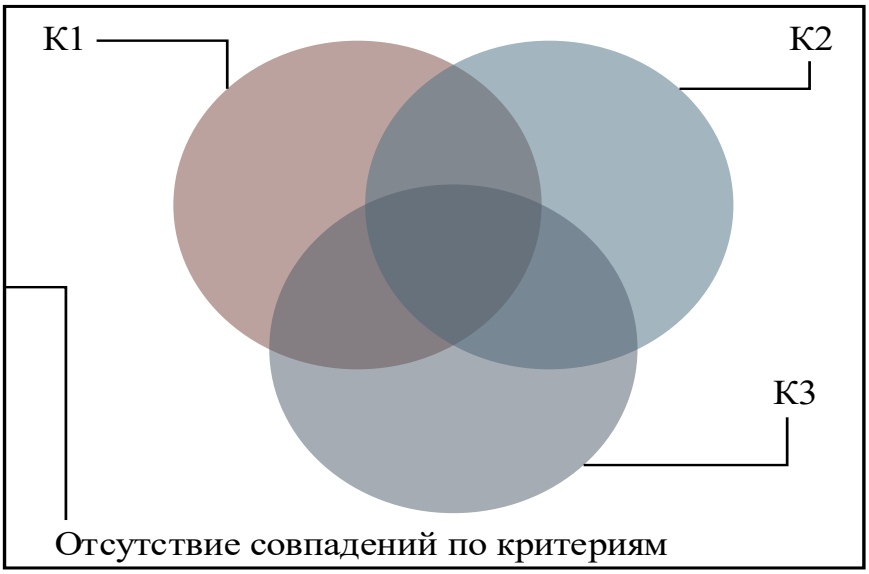


Рисунок 2.7 – Логическая диаграмма критериев интеллектуальной группировки

Критерий 1 (К1) – содержит текстовые данные пользователя и возможные отклонения в них. Категория риска: средний.

Критерий 2 (К2) – содержит медиа данные пользователя и возможные отклонения в них. Категория риска: средний.

Критерий 3 (К3) – содержит деструктивные сообщества пользователя и возможные участия в них. Категория риска: средний.

Пересечения критериев:

1. К1 и К2 – анализируются случаи, когда у пользователя одновременно наблюдаются отклонения в текстовых данных (К1) и медиа данных (К2). Категория риска: высокий.

2. К1 и К3 – оценивается сочетание подозрительных текстовых данных (К1) и участие в деструктивных сообществах (К3). Категория риска: высокий.

3. К2 и К3 – изучается связь между медиа данными (К2) и участием в деструктивных сообществах (К3). Категория риска: высокий.

4. К1 и К2 и К3 – есть отклонения в текстовых данных (К1), медиа данных (К2) и активность в деструктивных сообществах. Категория риска: критический.

Отсутствие совпадений по критериям определяется как низкая категория риска.

Предложенный метод позволяет выявлять новые формы деструктивного контента через мультимодальный анализ и интеллектуальную группировку.

На этапах реализации метода выполняется:

1. Обнаружение аномалий;
2. Кластеризация;
3. Экспертное оценивание;
4. Формирование класса «Z».

Класс «Z» — новая форма деструктивного поведения или не классифицируемые действия пользователей.

Метод выявляет противоречия между модальностями или не классифицируемые действия пользователей, далее данные группируются по схожим признакам. Новый кластер передается на анализ экспертам для подтверждения его деструктивной направленности. На основе экспертной оценки система дополняет классификатор новым классом [119, 127].

Схема на рисунке 2.8 демонстрирует процесс выявления нового класса.

Рисунок 2.8 – Схема выявления нового класса «Z»

Завершающий этап метода предусматривает представление результатов в структурированном виде, что обеспечивает удобство интерпретации результатов и их реализацию в интеллектуальных информационных системах. Формируются отчеты и рекомендации, которые содержат классифицированные группы категориальных данных.

2.3 Реализация метода обработки мультимодальных данных из сети интернет

Метод включает комплексный подход к сбору и обработке мультимодальных данных пользователей социальной сети, объединяющий 3 взаимосвязанных этапа анализа:

1. Сбор пользовательских данных;
2. Анализ данных;
3. Оценка рисков на основе мультимодальных критериев.

В рамках разработки метода приведено комплексное решение для сбора и обработки текстовых данных на примере классификации комментариев пользователей в социальной сети по категориям [28, 31, 35-37].

Текстовые данные в виде комментариев собраны из групп социальной сети ВКонтакте, общим объемом более 300 000 записей. Для обработки и классификации текстовых данных была задействована языковая модель Qwen2.5-7B.

Процесс обработки данных включал следующие ключевые этапы:

1. Подготовка данных;
2. Настройка и загрузка модели ИИ;
3. Классификация;
4. Категоризация.

Фрагмент кода, демонстрирующий первоначальный этап реализации классификации текстовых комментариев с использованием языковой модели Qwen2.5-7B на листинге 2.1.

Листинг 2.1 – Первоначальный этап реализации классификации

```
MODEL_NAME = "Qwen2.5-7B"
INPUT_FILE = "data/vk_comments.xlsx"
COMMENTS_COLUMN_NAME = "comments"
OUTPUT_DIR = "Результаты_Классификации"
OUTPUT_ALL_FILE = os.path.join (OUTPUT_DIR,
Все_комментарии_с_категориями.xlsx")
```

Продолжение листинга 2.1.

```
CATEGORIES = {
    "Распространение негатива": "negativity",
    "Саботаж": "sabotage",
    "Нарушение корпоративных норм": "corp_norms_violation",
    "Кибербуллинг (травля)": "cyberbullying",
    "Другие случаи": "other",
    "Ошибка классификации": "error"
}
```

На первоначальном этапе задаются основные параметры: указывается название используемой модели Qwen2.5-7B, путь к входному файлу «data/vk_comments.xlsx» с комментариями, название столбца «comments» с текстами комментариев, а также директория и имя файла для сохранения результатов.

Словарь «CATEGORIES» определяет категоризацию комментариев по классам:

1. Распространение негатива;
2. Саботаж;
3. Нарушение корпоративных норм;
4. Кибербуллинг (травля);
5. Другие случаи;
6. Ошибка классификации.

Такая структура позволяет гибко классифицировать типы деструктивного контента в текстах.

Итоговый файл результатов будет содержать все исходные комментарии с добавленными метками категорий, что позволит проводить последующий анализ классифицированных данных

На рисунке 2.9 представлен запуск языковой модели Qwen2.5-7B.

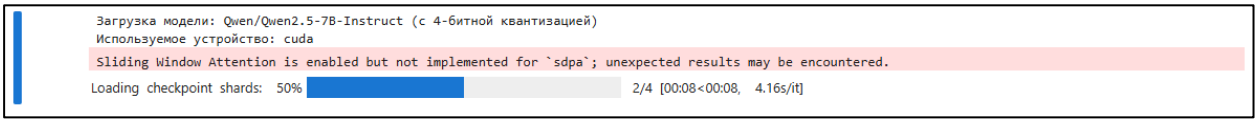


Рисунок 2.9 – Результат запуска языковой модели Qwen2.5-7B

Фрагмент кода, демонстрирующий сохранение результатов классификации текстовых комментариев на листинге 2.2.

Листинг 2.2 – Сохранение результатов классификации

```
print("Сохранение результатов...")

os.makedirs(OUTPUT_DIR, exist_ok=True)
results_df = pd.DataFrame(results)

if not results_df.empty:
    try:
        results_df.to_excel(OUTPUT_ALL_FILE, index=False, engine='openpyxl')
        print(f"Общий файл сохранен: {OUTPUT_ALL_FILE}")
    except Exception as e:
        print(f"Ошибка сохранения общего файла: {e}")

    category_counts = Counter(results_df['Category'])

    for category_name in CATEGORY_NAMES_RU:
        if category_name == "Ошибка классификации" and
category_counts.get(category_name, 0) == 0:
            continue

        category_df = results_df[results_df['Category'] == category_name]
        if not category_df.empty: # Проверяем еще раз, хотя count > 0 должен это
гарантировать
            output_category_file = os.path.join(OUTPUT_DIR, f"{category_name}.xlsx")
            try:
                category_df[['Comment']].to_excel(output_category_file, index=False, header=True,
engine='openpyxl')
            except Exception as e:
                print(f"Ошибка сохранения файла '{output_category_file}': {e}")

    print("Сохранение файлов по категориям завершено.")
```

Создается общий Excel-файл со всеми данными и их категориями, затем для каждой категории генерируются файлы с соответствующими данными.

После обработки всех категорий выводится уведомление об успешном завершении сохранения файлов по категориям.

На рисунке 2.10 представлен результат создания Excel-файлов и их названия в соответствии с категориями классов.

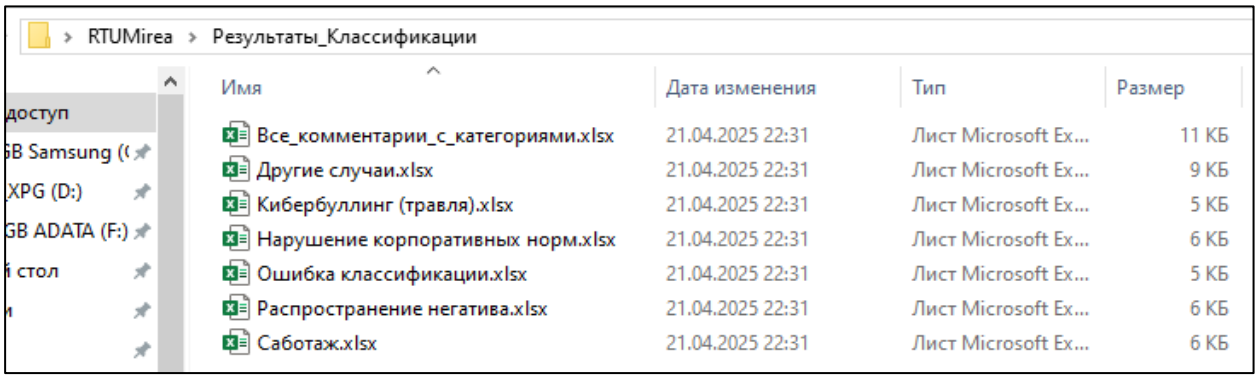


Рисунок 2.10 – Результат создания Excel-файлов с категориями классов

На рисунке 2.11 и рисунке 2.12 представлены примеры содержимого Excel-файлов.

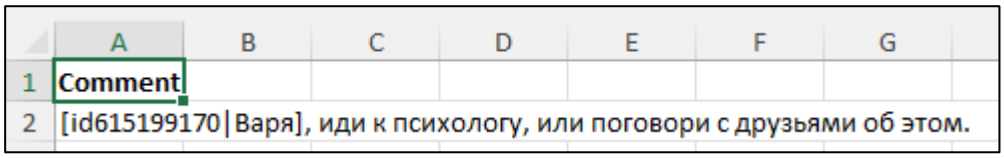


Рисунок 2.11 – Результат содержимого Excel-файла на примере одного из классов. Часть 1

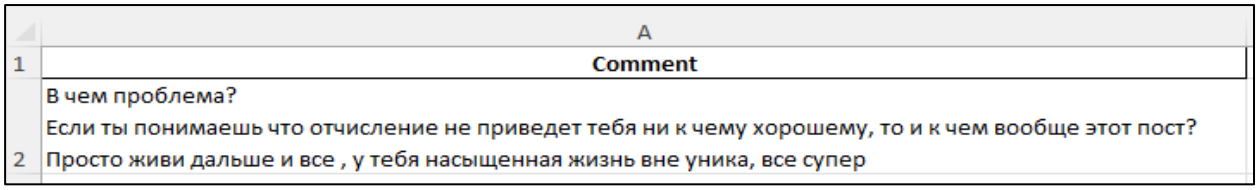
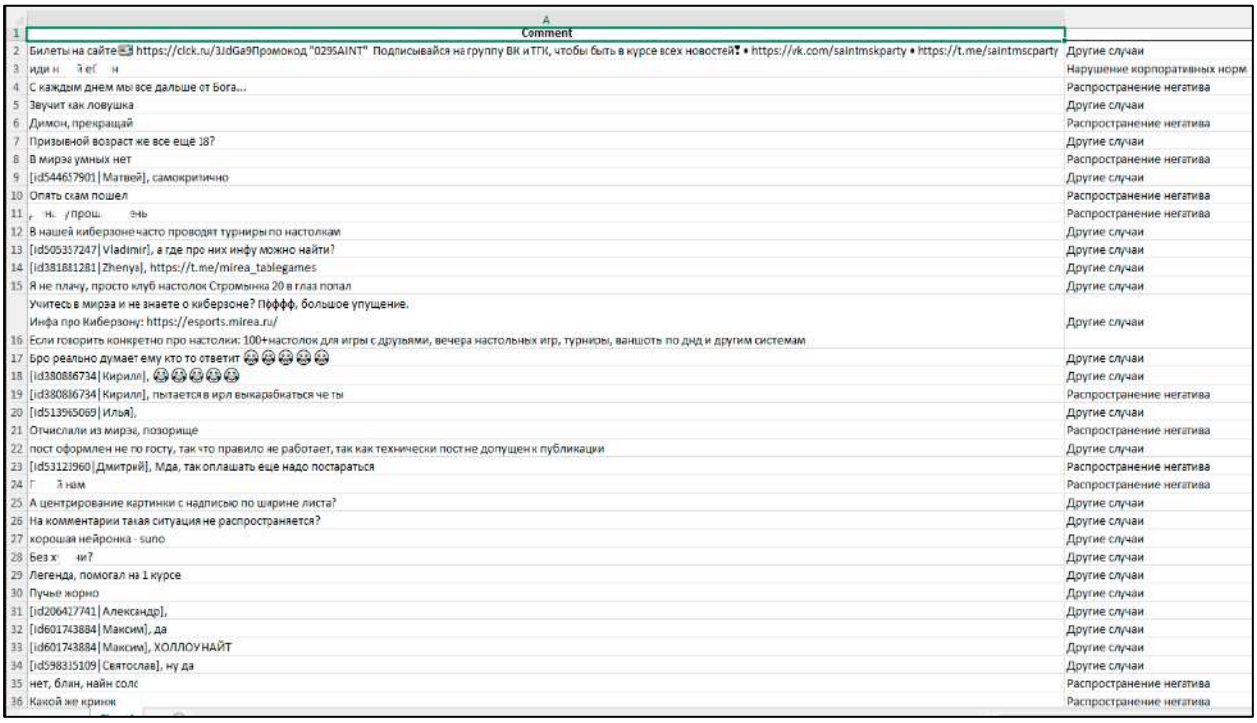


Рисунок 2.12 – Результат содержимого Excel-файла на примере одного из классов. Часть 2

На рисунке 2.13 представлен результат содержимого общего Excel-файла со всеми категориями.



	A	
1	Comment	
2	Билеты на сайте https://clck.ru/3JdGa9Промокод "0295AINT" Подписывайся на группу ВК и ТГК, чтобы быть в курсе всех новостей • https://vk.com/saintmskparty • https://t.me/saintmscparty	Другие случаи
3	иди н й еб н	Нарушение корпоративных норм
4	С каждым днем мы все дальше от Бога...	Распространение негатива
5	Звучит как ловушка	Другие случаи
6	Димон, прекращай	Распространение негатива
7	Призывной возраст же все еще 18?	Другие случаи
8	В мирэа умных нет	Распространение негатива
9	[id544657901|Матвей], самокритично	Другие случаи
10	Опять скам пошел	Распространение негатива
11	, н. прош ень	Распространение негатива
12	В нашей киберзоне часто проводят турниры по настолкам	Другие случаи
13	[id505357247|Vladimir], а где про них инфу можно найти?	Другие случаи
14	[id381881281|Zhenya], https://t.me/mirea_tablegames	Другие случаи
15	Я не плачу, просто клуб настолок Стромынка 20 в глаз попал	Другие случаи
	Учитесь в мирэа и не знаете о киберзоне? Пффф, большое упущение. Инфа про Киберзону: https://esports.mirea.ru/	Другие случаи
16	Если говорить конкретно про настолки: 100+настолок для игры с друзьями, вечера настольных игр, турниры, ваншоты по днд и другим системам	
17	Бро реально думает ему кто то ответит 😭😭😭😭😭	Другие случаи
18	[id380886734|Кирилл], 😭😭😭😭😭	Другие случаи
19	[id380886734|Кирилл], пытается в ирл выкарабкаться че ты	Распространение негатива
20	[id513965069|Илья],	Другие случаи
21	Отчислали из мирэа, позорище	Распространение негатива
22	пост оформлен не по госту, так что правило не работает, так как технически пост не допущен к публикации	Другие случаи
23	[id53121960|Дмитрий], Мда, так оплашать еще надо постараться	Распространение негатива
24	Г й нам	Распространение негатива
25	А центрирование картинки с надписью по ширине листа?	Другие случаи
26	На комментарии такая ситуация не распространяется?	Другие случаи
27	хорошая нейронка - suno	Другие случаи
28	Без х ни?	Другие случаи
29	Легенда, помогал на 1 курсе	Другие случаи
30	Пучье жорно	Другие случаи
31	[id206427741|Александр],	Другие случаи
32	[id601743884|Максим], да	Другие случаи
33	[id601743884|Максим], ХОЛЛОУ НАЙТ	Другие случаи
34	[id598315109|Святослав], ну да	Другие случаи
35	нет, блин, найн солс	Распространение негатива
36	Какой же кринж	Распространение негатива

Рисунок 2.13 – Результат содержимого общего Excel-файла со всеми категориями

Фрагмент кода, демонстрирующий формирование статистики классификации текстовых комментариев на листинге 2.3.

Листинг 2.3 – Формирование статистики классификации

```
print("\n--- Статистика по категориям ---")
    total_comments_processed = len(results_df)
    sorted_categories = sorted(category_counts.items(), key=lambda item: item[1],
reverse=True)

    for category_name, count in sorted_categories:
        if category_name == "Ошибка классификации" and count == 0:
            continue
        percentage = (count / total_comments_processed) * 100 if total_comments_processed > 0
else 0
        print(f"{category_name} - {percentage:.2f}% | (Содержит {count} комментариев)")

else:
    print("Нет результатов для сохранения и отображения статистики.")

print("--- Работа завершена! ---")
```

Данный фрагмент кода выполняет финальный этап обработки результатов классификации комментариев и формирует статистику. Статистика выводится в виде процентного соотношения и абсолютного количества данных по каждой категории в порядке убывания. В случае отсутствия результатов или ошибок при сохранении выводятся соответствующие уведомления. Процесс завершается сообщением о завершении работы.

На рисунке 2.14 представлен результат классификации текстовых комментариев по их категориям и их статистика.

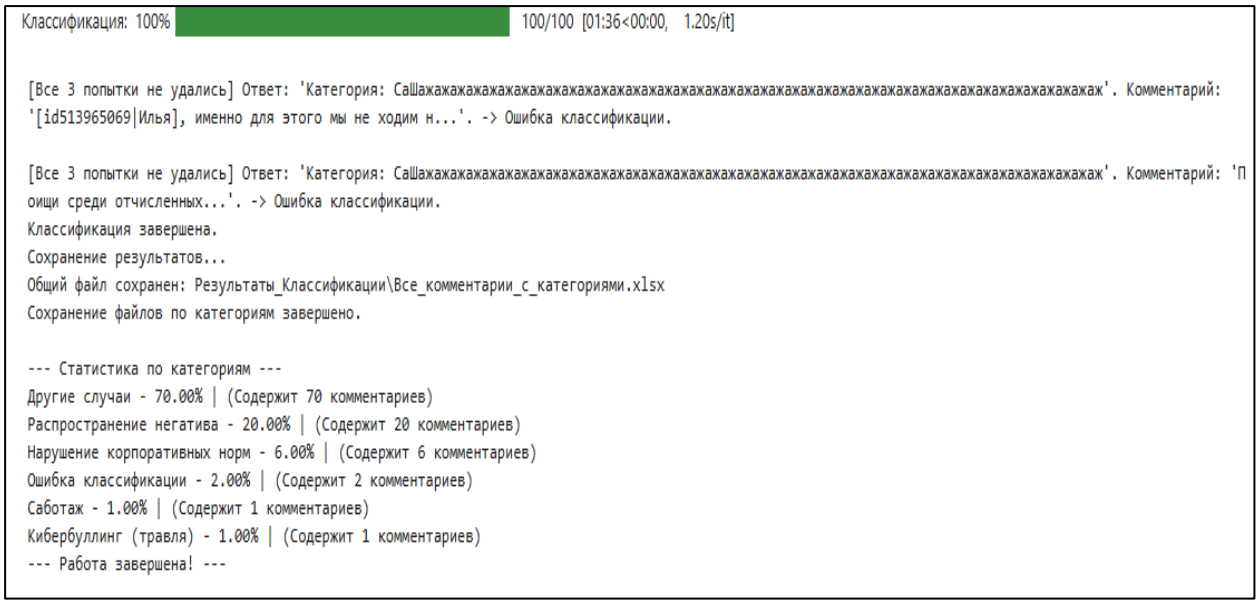


Рисунок 2.14 – Результат классификации на примере комментариев и их категорий

В рамках разработки метода приведено комплексное решение для сбора и обработки текстовых данных и медиа данных через раздельные модули с последующей консолидацией выводов для выявления потенциально опасного контента.

Фрагмент кода, демонстрирующий обработку видео с YOLO отображен на листинге 2.4.

Листинг 2.4 – Обработка видео с YOLO

```
cap = cv2.VideoCapture(input_path)
fps = cap.get(cv2.CAP_PROP_FPS)
frame_width = int(cap.get(cv2.CAP_PROP_FRAME_WIDTH))
frame_height = int(cap.get(cv2.CAP_PROP_FRAME_HEIGHT))
cap.release()

out = cv2.VideoWriter(output_path, cv2.VideoWriter_fourcc(*'mp4v'), fps, (frame_width,
frame_height))
results_gen = model.predict(source=input_path, stream=True,
conf=MEDIA_CONFIDENCE_THRESHOLD, verbose=False)
for res in results_gen:
   out.write(draw_custom_boxes(res, res.orig_img))
out.release()
```

Данный фрагмент демонстрирует обработку видеофайлов в реальном времени. Программа на вход получает характеристики видео (FPS, разрешение), затем создает видеопоток для записи результатов. Модель YOLO анализирует каждый кадр и записывает в выходной файл кадры с обнаруженными объектами.

Фрагмент кода, демонстрирующий обработку текста с Qwen2.5-7B отображен на листинге 2.5.

Листинг 2.5 – Обработка текста с Qwen2.5-7B

```
def process_text():
   print(f"\n{C_HEADER}")
   start_time = time.time()

   model, tokenizer = initialize_ai_model()
   if not model: return
      try:
      with open(TEXT_INPUT_FILE, "r", encoding="utf-8") as f: all_lines = [l.strip() for l in f
if l.strip()]
      if not all_lines: print(f"{C_WARN}Входной файл '{TEXT_INPUT_FILE}' пуст.");
return
   except Exception:
      print(f"{C_ERROR}Ошибка: Входной файл не найден или не читается:
{TEXT_INPUT_FILE}"); return

   os.makedirs(TEXT_OUTPUT_DIR, exist_ok=True)
   with open(TEXT_OUTPUT_FILE, 'w', encoding='utf-8') as f: pass
```

Данный фрагмент выполняет анализ текстовых данных на предмет деструктивного контента с использованием модели Qwen2.5-7B.

Для обработки используется механизм пакетной отправки запросов к языковой модели. Все обнаруженные отклонения сохраняются в выходной файл, на основе которого выводится сводная статистика, включая общее количество проанализированных строк, число найденных нарушений и время выполнения задачи.

Фрагмент кода, демонстрирующий комбинированный запуск модулей анализа (Текст + Медиа) отображен на листинге 2.6.

Листинг 2.6 – Комбинированный запуск модулей анализа (Текст + Медиа)

```
def run_combined_analysis():
    """Функция для комплексного анализа медиа и текстовых данных"""
    print(f"{C_HEADER}=== ЗАПУСК КОМБИНИРОВАННОГО АНАЛИЗА ===")
    start_time = time.time()

    print(f"\n{C_HEADER}[1/2] ЗАПУСК МЕДИА-АНАЛИЗАТОРА")
    media_start = time.time()
    process_media()
    media_time = time.time() - media_start
    print(f"{C_INFO}Медиа-анализ выполнен за {media_time:.2f} сек.")

    print(f"\n{C_HEADER}[2/2] ЗАПУСК ТЕКСТОВОГО АНАЛИЗАТОРА")
    text_start = time.time()
    process_text()
    text_time = time.time() - text_start
    print(f"{C_INFO}Текстовый анализ выполнен за {text_time:.2f} сек.")

    total_time = time.time() - start_time
    print(f"\n{C_SUCCESS}=== ИТОГИ КОМПЛЕКСНОГО АНАЛИЗА ===")
    print(f"{C_INFO}Общее время выполнения: {total_time:.2f} сек.")
    print(f"{C_INFO}Медиафайлы: {media_time:.2f} сек.")
    print(f"{C_INFO}Текстовые данные: {text_time:.2f} сек.")
    print(f"{C_HEADER}="*50 + "\n")
```

Данный фрагмент выполняет последовательный запуск независимых модулей анализа контента.

Первоначальным этапом запускается модуль медиа-анализа, который обрабатывает графические и видео материалы с использованием YOLO-модели.

После завершения медиа-анализа следующим этапом автоматически запускается языковая модель Qwen2.5-7B для анализа текстовых данных.

Технической особенностью реализации является независимость модулей друг от друга, они могут выполняться как совместно, так и по отдельности.

В рамках разработки метода приведено комплексное решение для сбора и обработки информации о пользователях и их активности в группах с возможностью выявления потенциально опасного контента.

Решение включает в себя 3 модуля:

1. Сбор информации об участниках указанной группы или чата;
2. Сбор групп пользователей;
3. Анализ групп и выявление пользователей, состоящих в деструктивных сообществах.

На рисунке 2.15 представлен чат, на примере которого совершается сбор информации о пользователях.

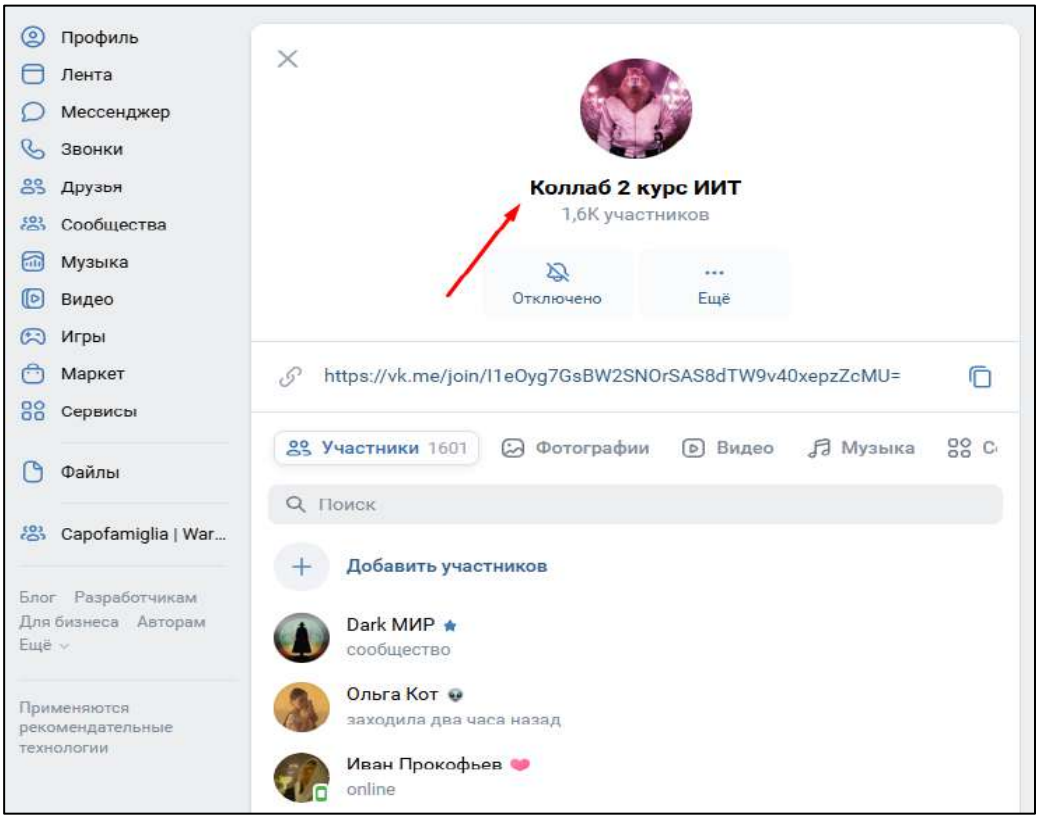


Рисунок 2.15 – Пример чата в социальной сети для сбора информации о пользователях

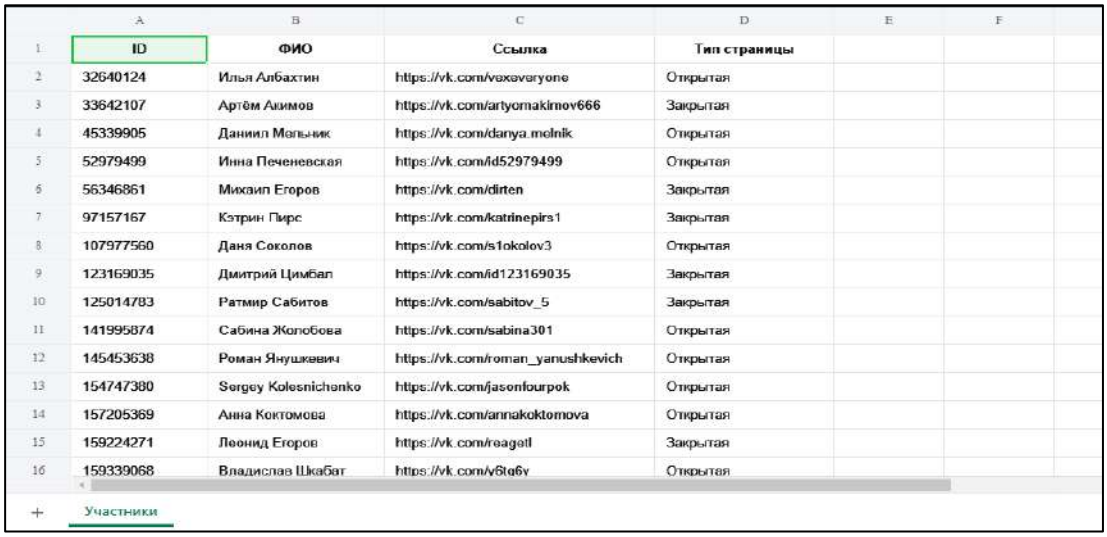
Фрагмент кода, демонстрирующий процесс сбора списка всех участников группы отображен на листинге 2.7.

Листинг 2.7 – Процесс сбора списка всех участников группы

```
def get_entity_members_raw(entity_id_str):
    raw_members_list = []
    offset = 0
    is_chat_mode = int(entity_id_str) >= 2000000000

    while True:
        params = {
            'group_id': entity_id_str,
            'count': 1000,
            'offset': offset,
            'fields': 'is_closed, screen_name, deactivated'
        }
        response_data = get_vk_api('groups.getMembers', params)

        if not response_data:
            break

        current_batch = response_data.get('items', [])
        if not current_batch:
            break

        raw_members_list.extend(current_batch)
        offset += len(current_batch)
        time.sleep(0.34)  # Задержка для соблюдения лимитов API

    return raw_members_list
```

Данный фрагмент демонстрирует получение списка всех пользователей группы.

На рисунке 2.16 представлен результат сбора информации о пользователях на примере чата в социальной сети.



	A	B	C	D	E	F
1	ID	ФИО	Ссылка	Тип страницы		
2	32640124	Илья Албахтин	https://vk.com/vexeveryone	Открытая		
3	33642107	Артём Акимов	https://vk.com/artyomakimov666	Закрытая		
4	45339905	Даниил Мельник	https://vk.com/danya.molnik	Открытая		
5	52979499	Инна Печеневская	https://vk.com/id52979499	Открытая		
6	56346861	Михаил Егоров	https://vk.com/dirten	Закрытая		
7	97157167	Кэтрин Пирс	https://vk.com/katrinepirs1	Закрытая		
8	107977560	Даня Соколов	https://vk.com/s1okolov3	Открытая		
9	123169035	Дмитрий Цимбал	https://vk.com/id123169035	Закрытая		
10	125014783	Ратмир Сабитов	https://vk.com/sabitov_5	Закрытая		
11	141995874	Сабина Жолобова	https://vk.com/sabina301	Открытая		
12	145453638	Роман Янушкевич	https://vk.com/roman_yanushkevich	Открытая		
13	154747380	Sergey Kolesnichenko	https://vk.com/jasonfourpok	Открытая		
14	157205369	Анна Коктомова	https://vk.com/annakoktomova	Открытая		
15	159224271	Леонид Егоров	https://vk.com/reagatl	Закрытая		
16	159339068	Владислав Шкабат	https://vk.com/v6tq6v	Открытая		

+ Участники

Рисунок 2.16 – Результат сбора информации о пользователях на примере чата в социальной сети

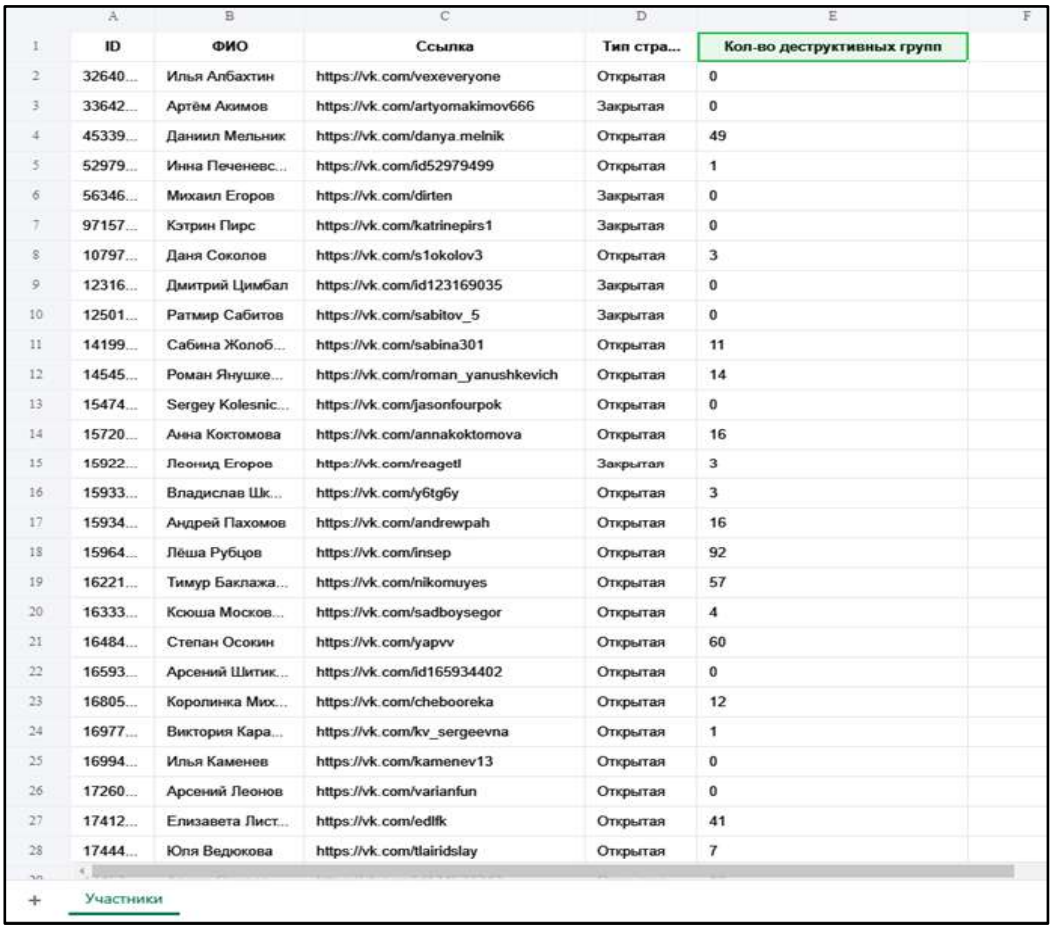
Фрагмент кода, демонстрирующий процесс анализа деструктивных групп отображен на листинге 2.8.

Листинг 2.8 – Процесс анализа деструктивных групп

```
def run_group_analysis():
    destructive_group_lines_set = set()
    with open(BAD_GROUPS_REFERENCE_FILE, 'r') as f:
        for line in f:
            if line.strip() and not line.startswith("#"):
                destructive_group_lines_set.add(line.strip())

    for user_data_row in users_data:
        user_groups_file = os.path.join(user_dir, "groups.txt")
        with open(user_groups_file, 'r') as ugf:
            for group_line in ugf:
                if group_line.strip() in destructive_group_lines_set:
                    user_data_row['Кол-во деструктивных групп'] += 1
                    break
```

Данный фрагмент демонстрирует анализ групп пользователей на предмет их принадлежности к деструктивным сообществам. Результаты данного анализа применяются для классификации пользователей по уровню риска.

На рисунке 2.17 представлен результат по количеству деструктивных групп у пользователей на примере чата в социальной сети.



	A	B	C	D	E	F
1	ID	ФИО	Ссылка	Тип стра...	Кол-во деструктивных групп	
2	32640...	Илья Албахтин	https://vk.com/vexeveryone	Открытая	0	
3	33642...	Артём Акимов	https://vk.com/artyomakimov666	Закрытая	0	
4	45339...	Даниил Мельник	https://vk.com/danya.melnik	Открытая	49	
5	52979...	Инна Печеневс...	https://vk.com/id52979499	Открытая	1	
6	56346...	Михаил Егоров	https://vk.com/dirten	Закрытая	0	
7	97157...	Кэтрин Пирс	https://vk.com/katrinepirs1	Закрытая	0	
8	10797...	Даня Соколов	https://vk.com/s1okolov3	Открытая	3	
9	12316...	Дмитрий Цимбал	https://vk.com/id123169035	Закрытая	0	
10	12501...	Ратмир Сабитов	https://vk.com/sabitov_5	Закрытая	0	
11	14199...	Сабина Жолоб...	https://vk.com/sabina301	Открытая	11	
12	14545...	Роман Янушке...	https://vk.com/roman_yanushkevich	Открытая	14	
13	15474...	Sergey Kolesnic...	https://vk.com/jasonfourpok	Открытая	0	
14	15720...	Анна Коктомова	https://vk.com/annakoktomova	Открытая	16	
15	15922...	Леонид Егоров	https://vk.com/reagetl	Закрытая	3	
16	15933...	Владислав Шк...	https://vk.com/y6tg6y	Открытая	3	
17	15934...	Андрей Пахомов	https://vk.com/andrewpah	Открытая	16	
18	15964...	Лёша Рубцов	https://vk.com/insep	Открытая	92	
19	16221...	Тимур Баклажа...	https://vk.com/nikomuyes	Открытая	57	
20	16333...	Ксюша Москов...	https://vk.com/sadboysegor	Открытая	4	
21	16484...	Степан Осокин	https://vk.com/yapvv	Открытая	60	
22	16593...	Арсений Шитик...	https://vk.com/id165934402	Открытая	0	
23	16805...	Королинка Мих...	https://vk.com/chebooreka	Открытая	12	
24	16977...	Виктория Кара...	https://vk.com/kv_sergeevna	Открытая	1	
25	16994...	Илья Каменев	https://vk.com/kamenev13	Открытая	0	
26	17260...	Арсений Леонов	https://vk.com/varianfun	Открытая	0	
27	17412...	Елизавета Лист...	https://vk.com/edlfk	Открытая	41	
28	17444...	Юля Ведюкова	https://vk.com/tlairidslay	Открытая	7	

+ Участники

Рисунок 2.17 – Результат по количеству деструктивных групп у пользователей на примере чата в социальной сети

В рамках разработки метода как одного из этапов приведена интеллектуальная группировка.

В контексте разрабатываемом методе интеллектуальная группировка данных включает в себя объединение модулей:

1. Текстовый анализ (классификация комментариев на деструктивные и не деструктивные);
2. Медиа анализ (обнаружение запрещенных объектов в изображениях и видео);
3. Социальный анализ (выявление участия пользователей в деструктивных группах).

Для подтверждения эффективности разработанного метода обработки мультимодальных данных было проведено тестирование на одном из чатов студентов Института информационных технологий РТУ МИРЭА.

Под «сообществом» в данном контексте понимается сообщество в социальной сети Интернет, в котором состоит пользователь. Общее количество пользователей составило 2000. Для анализа деструктивной активности рассматривались их подписки и участие в сообществах. Каждый пользователь в среднем состоит в 25-26 сообществах, общее количество для проверки составило 51000 сообществ.

В таблице 2.11 представлен сравнительный анализ эффективности методов выявления деструктивных групп пользователей между существующим и разработанным.

Таблица 2.11 – Сравнительный анализ эффективности методов выявления деструктивных групп пользователей

Критерий	**Существующий подход**	**Разработанный метод**	**Экономия / Ускорение**
Объем данных (2000 пользователей)	Выборочная проверка (50-100 пользователей)	Все пользователи	Полный охват пользователей
Общее время обработки (51000 сообществ)	142 ч	1,14 ч	В 125 раз
Скорость обработки (1 сообщество)	10 сек	0,08 сек	
Результат для эксперта	Список групп для ручной проверки	Готовый отчет: пользователь и количество деструктивных групп	Структурированный результат для эксперта

Данные в таблице демонстрируют, что разработанный метод позволяет не только обеспечить полный охват пользователей, но и сокращает время обработки деструктивных групп в 125 раз.

В качестве объекта внедрения выбрана действующая система анализа цифровых взаимодействий сотрудников в ООО «НПК «КарбонГрупп» (акт о внедрении результатов диссертационного исследования в приложении диссертации).

В таблице 2.12 приведен пример определения уровня угрозы по категориям риска, включающие набор критериев: содержание текста, тип медиаконтента и активность пользователя в социальных группах.

Таблица 2.12 – Критерии интеллектуальной группировки для оценки риска

Категория риска	**Критерии**
Критический	отклонения в тексте + запрещенный контент в медиа + участие в деструктивных группах
Высокий	отклонения в тексте + подозрительный контент в медиа + участие в деструктивных группах
Средний	отклонения в тексте + нет опасного контента в медиа + участие в нейтральных группах
Низкий	нейтральный текст + безопасный контент в медиа + участие в нейтральных группах

Результаты применения интеллектуальной группировки на примере пользователей отражены в таблице 2.13.

Таблица 2.13 – Результаты применения метода на примере пользователей

Пользователь	**Текст**	**Медиа**	**Группы**	**Категория риска**
ID376235	Саботаж	Оружие	12 деструктивных	Критический
ID189624	Нейтральный	Безопасно	Нейтральные	Низкий

В приведенной таблице показано, что итоговая категория риска формируется за счет комплексного анализа. Пользователям присваивается

критический уровень риска, в результате выявления деструктивных признаков во всех трех модальностях.

На рисунке 2.18 представлено сравнение унимодального и мультимодального анализа по качеству оценки риска

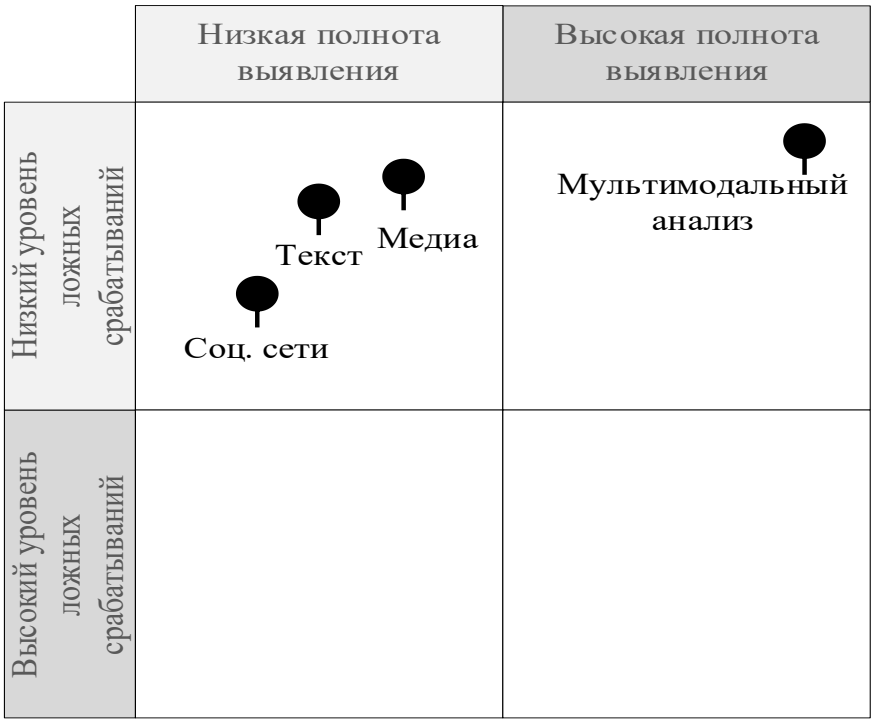


Рисунок 2.18 – Сравнение унимодального и мультимодального анализа по качеству оценки риска

Результаты применения унимодального и мультимодального анализа по качеству оценки риска отражены в таблице 2.14.

Таблица 2.14 – Результаты применения унимодального и мультимодального анализа по качеству оценки риска

Пользователь	**Текст**	**Медиа**	**Группы**	**Унимодальный анализ**	**Мультимодальный анализ**
ID376…	Саботаж	Оружие	12 деструктивных	Высокий	Критический
ID189…	Нейтральный	Безопасно	Нейтральные	Низкий	Низкий
ID952…	Дезинформация	Безопасно	Нейтральные	Высокий	Средний

Представленная таблица демонстрирует, что мультимодальный анализ обеспечивает качественную оценку посредством комплексного учета всех доступных данных о пользователе.

Данное исследование расширяет мультимодальность цифрового следа за счет перехода от унимодального анализа разрозненных данных к комплексному.

Таким образом, разработанный метод включает последовательные этапы анализа данных, а ее структура позволяет выявлять и классифицировать потенциальные угрозы.

2.4 Выводы по главе

Во второй главе представлен комплексный подход обработки мультимодальных данных.

Разработан метод обработки мультимодальных данных из сети Интернет для интеллектуальных систем, объединяющая методы обработки текстовых данных, медиа данных и социальной активности пользователей.

Предложенный подход включает интеллектуальную группировку данных и автоматизированное аннотирование за счет моделей Qwen2.5-7B для текстовых данных и YOLO для медиа данных.

Ключевые результаты, полученные в данной главе, включают:

1. Систематизацию методов обработки мультимодальных данных с обоснованием выбора моделей Qwen2.5-7B и YOLO как наиболее эффективных решений для соответствующих типов данных.

2. Разработку метода обработки мультимодальных данных из взаимодополняющих компонентов: текстовые данные, медиа данные и социальная активность пользователей, объединение которых обеспечивает комплексную оценку угроз, что значительно сокращает время выявления пользователей, состоящих в деструктивных сообществах, и расширяет мультимодальность исследования цифрового следа за счет комплексного анализа данных из сети Интернет;

3. Концепция механизма формирования класса «Z» для потенциально неизвестных случаев деструктивного поведения.

4. Установлены критерии интеллектуальной группировки данных по уровням угрозы с учетом мультимодальных признаков.

Полученные результаты, представленные во второй главе, создают прочную основу для практического применения предложенных решений в различных областях, включая мониторинг социальных сетей, обеспечение безопасности и модерацию контента.

ГЛАВА 3 КРОСС-МОДАЛЬНЫЙ ВЕРОЯТНОСТНЫЙ МЕТОД КЛАССИФИКАЦИИ ЦИФРОВОЙ ОБРАБОТКИ АУДИО, ТЕКСТОВЫХ ДАННЫХ, ФОТО И ВИДЕОИЗОБРАЖЕНИЙ КОНТЕНТА

3.1 Постановка задачи разработки кросс-модального вероятностного метода классификации

В данной главе рассматривается метод, сочетающий цифровую обработку контента и его контекста, с последующим вычислением условной вероятности для выявления форм поведения пользователей.

Социальные сети и цифровые платформы представляют собой сложную мультимодальную среду, где аудио, текст, фото и видео изображения образуют единый поток. Деструктивное поведение пользователей часто проявляется через сочетание модальностей, что приводит к новым подходам его выявления [29, 30].

Предлагаемый кросс-модальный вероятностный метод основан на анализе взаимосвязей между аудио, текстовыми и визуальными компонентами контента, что позволяет выявлять не только явные, но и скрытые формы отклонений в поведении.

На рисунке 3.1 демонстрируется пример входных данных рассматриваемых мультимодальных объектов контента.

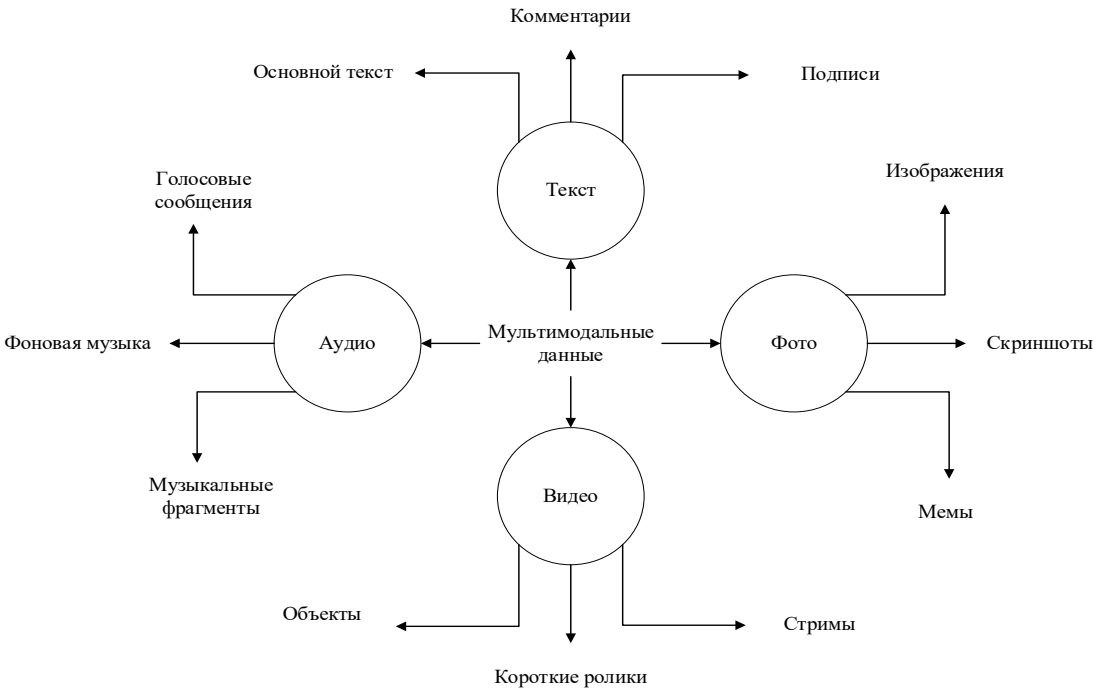


Рисунок 3.1 – Пример исходных данных мультимодальных объектов контента

В контексте разрабатываемого подхода формы деструктивного контента представляют собой мультимодальные данные с явным или скрытым признаком отклонения в поведении пользователей [60-64]. Для решения данной проблемы предлагается кросс-модальный вероятностный метод классификации, основанный на анализе контента и контекста [72, 75]. Далее в исследовании представлены примеры маркеров деструктивности для каждой модальности.

В таблице 3.1 продемонстрированы примеры маркеров деструктивности аудиоконтента.

Таблица 3.1 – Маркеры деструктивности на примере аудиоконтента

Аудиоданные	**Примеры деструктивности**
Голосовые сообщения	Повышенная громкость, агрессивная интонация
Фоновые звуки	Звуки выстрелов, крики
Музыкальные фрагменты	Экстремистские тексты в музыкальных произведениях

В таблице 3.2 продемонстрированы примеры маркеров деструктивности текстового контента.

Таблица 3.2 – Маркеры деструктивности на примере текстового контента

Текстовые данные	**Примеры деструктивности**
Основной текст	Угрозы, призывы к насилию, экстремистские лозунги, дискриминационная лексика
Комментарии	Троллинг, кибербуллинг, спам, координированные атаки на пользователей
Подписи	Двусмысленные подписи со скрытыми угрозами, запрещенные материалы

В таблице 3.3 продемонстрированы примеры маркеров деструктивности видеоконтента.

Таблица 3.3 – Маркеры деструктивности на примере видеоконтента

Видеоданные	**Примеры деструктивности**
Короткие ролики	Опасные челленджи, демонстрация насилия, деструктивные призывы
Объекты	Запрещенная символика, оружие, опасные предметы в кадре
Стримы	Прямые трансляции противоправных действий, вербальная агрессия в реальном времени

В таблице 3.4 продемонстрированы примеры маркеров деструктивности фотоизображений контента.

Таблица 3.4 – Маркеры деструктивности на примере фотоизображений контента

Фотоизображения	Примеры деструктивности
Мемы	Мемы с экстремистским подтекстом, оскорбительные мемы, дезинформация
Скриншоты	Фейковые переписки, поддельные документы, компрометирующие материалы
Изображения	Графические сцены насилия, запрещенная символика, измененные фото с вредоносным контекстом

Таким образом, каждая модальность контента требует особого подхода к выявлению деструктивных маркеров, что подчеркивает необходимость разрабатываемого подхода [20-22, 71].

В условиях стремительного роста объемов пользовательского контента и усложнения форм цифровых коммуникаций перед платформами встает комплекс задач обработки контента [43, 45-48].

Разработка кросс-модального вероятностного метода включает решение следующих ключевых задач:

1. Выявление сложных форм деструктивного поведения;
2. Обработка контента в режиме реального времени;
3. Снижение ложных срабатываний;
4. Обнаружение новых форм угроз.

Данный подход применим в социальных сетях, чат-платформах и других коммуникативных площадках, примеры решаемых проблем и платформ продемонстрированы в таблице 3.5.

Таблица 3.5 – Применение метода на примере цифровых платформ

Тип платформы	Примеры решаемых проблем
Социальные сети	Изображения с двойным смыслом Координированные атаки Фейковые новости
Мессенджеры	Скрытые угрозы в аудио Фишинг в чатах Буллинг в группах

Продолжение таблицы 3.5

Игровые платформы	Токсичность в реальном времени Выявление нарушителей правил Мошенничество
Форумы/Блоги	Спам-атаки Дезинформация Деструктивные обсуждения
Видеохостинги	Опасные челленджи Деструктивные комментарии Нелегальный контент

Далее в исследовании представлена концепция кросс-модального вероятностного метода классификации.

3.2 Концепция кросс-модального вероятностного метода классификации

Разрабатываемый подход основан на двухэтапном анализе, где сначала выявляются характерные признаки контента и определение нового класса деструктивности «Z», а затем рассчитывается условная вероятность деструктивности.

На рисунке 3.2 продемонстрированы этапы разрабатываемого метода.

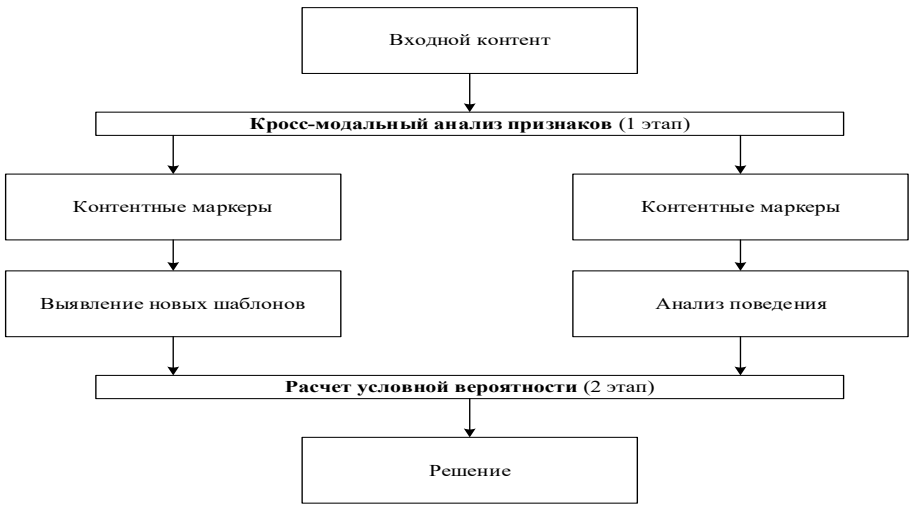


Рисунок 3.2 – Схема этапов кросс-модального вероятностного метода классификации

На первом этапе выполняется кросс-модальный анализ контента и контекста, где учитываются не только сами данные, но и их взаимосвязи. Кросс-модальный – подход к обработке данных, отличается от существующих унимодальных методов способностью анализировать и выявлять взаимосвязи между различными типами контента [73]. В контексте разрабатываемого метода кросс-модальный анализ демонстрирует существенные преимущества, представленные в таблице 3.6.

Таблица 3.6 – Сравнение кросс-модального анализа и унимодальных методов

Критерий	**Кросс-модальный анализ**	**Существующие унимодальные методы**
Полнота данных	Анализ всех компонент контента (аудио, текст, фото и видео)	Анализ только одной модальности
Точность	Снижение ложных срабатываний за счет проверки контекста	Высокий риск ошибок из-за отсутствия контекста
Гибкость	Обнаружение скрытых паттернов	Высокий риск ошибок выявления скрытых угроз
Адаптивность	Выявление новых форм деструктивности (класс «Z»)	Постоянное обновление моделей для новых угроз

Для текстовых данных используются NLP-модели, способные выявлять токсичность, агрессивную лексику и скрытые угрозы. Аудиоданные обрабатываются нейросетевыми архитектурами для классификации эмоциональной окраски речи. Фото и видео данные анализируются с помощью алгоритмов детекции объектов и распознавания действий, что позволяет обнаружить деструктивное поведение и символы [44, 51].

Основное преимущество кросс-модального анализа заключается в его комплексности. В отличие от существующих методов, осуществляется

двухэтапная классификация контента за счет оценки вероятности проявления деструктивного поведения пользователя [74].

В распространяющемся контенте постоянно появляются новые формы деструктивного контента, которые необходимо обнаруживать в режиме реального времени. Особую сложность представляет класс «Z» – не классифицируемые или новые, ранее неизученные виды вредоносного контента.

В рамках данного исследования критерий отнесения к деструктивному поведению является не внешним правилом, а внутренним свойством обучающей выборки. Граница между деструктивным и не деструктивным контентом проводится: на этапе обучения через разметку данных или на этапе классификации по сходству эталонных примеров из обучающей выборки. Вектор признаков X формируется как совокупность контентных и контекстных признаков, фрагменты которых для различных модальностей приведены в таблице 3.7.

Таблица 3.7 – Фрагменты контентных и контекстных признаков

Тип контента	**Контентные признаки**	**Контекстные признаки**
Текст	Токсичная лексика, угрозы, угрозы, деструктивные призывы и лозунги	Аномальная активность в ночное время, высокая частота сообщений, координированные действия пользователей
Аудио	Крики, ненормативная лексика, агрессивная интонация, угрозы	Фоновые звуки (выстрелы, гипноз), неестественные паузы или модификации голоса
Видео	Демонстрация насилия, опасные челленджи, запрещенная символика, противоправные действия, дипфейки	Аномальная длительность роликов, повторяющиеся паттерны в разных видео от одного автора, признаки монтажа или глубокой обработки
Изображения	Символика экстремизма, запрещенная атрибутика	Признаки отредактированного фото, неестественные цветовые оттенки или следы обработки

На втором этапе осуществляется классификация на основе условной вероятности с учетом результатов контентного и контекстного анализа.

Байесовский классификатор был выбран для классификации на втором этапе по нескольким ключевым причинам.

Во-первых, данный классификатор осуществляет качественную вероятностную интерпретацию результатов, что важно в контексте разрабатываемого метода.

Во-вторых, классификатор эффективно работает с редкими событиями, например, с маркерами деструктивного поведения, благодаря использованию априорных вероятностей.

В-третьих, демонстрирует хорошую производительность на примере небольших обучающих выборках, что актуально для новых форм деструктивного контента в контексте разрабатываемого метода.

В таблице 3.8 приведены примеры методов классификации для задач модерации контента.

Таблица 3.8 – Сравнение методов классификации для задач модерации контента

Критерий	**Байесовский классификатор**	**Деревья решений**	**Нейронные сети**
Интерпретируемость	Высокая (точные формулы вероятностей)	Средняя (важность признаков)	Низкая
Работа с редкими классами	Высокая (априорные вероятности)	Средняя (необходима настройка)	Средняя (зависит от архитектуры)
Вычислительная сложность	Низкая (быстрые расчеты)	Средняя/высокая (для ансамблей)	Очень высокая
Адаптивность	Высокая (легкое обновление)	Средняя	Низкая (требует переобучения)

Для задачи метода классификации, где на втором этапе требуется именно вероятностная оценка с возможностью объяснения решений, Байесовский

подход является оптимальным между точностью, интерпретируемостью и эффективностью.

На втором этапе метода система переходит к объектно-вероятностной классификации, которая формализует дальнейший процесс принятия решений о деструктивном поведении через взаимосвязь мультимодальных признаков.

Каждый контент-объект рассматривается как динамическая система признаков.

Основная формула для расчета вероятности деструктивности:

$$P(Z|X) = \frac{P(X|Z) \times P(Z)}{P(X)}, \quad (3.1)$$

где, P(Z|X) – вероятность, что контент относится к классу деструктивности Z при данных признаков X, P(X|Z) – вероятность наблюдения признаков X для класса Z, P(Z) – базовая распространенность класса Z, P(X) – общая вероятность признаков X.

В таблице 3.9 представлены компоненты формулы вероятностной классификации.

Таблица 3.9 – Компоненты формулы вероятностной классификации

Обозначение	**Название**	**Описание**	**Как вычисляется**
P(Z|X)	Апостериорная вероятность	Вероятность, что контент относится к классу Z при наблюдаемых признаках X	Рассчитывается по формуле Байеса
P(X|Z)	Правдоподобие	Вероятность наблюдения признаков X для класса Z	Статистика по обучающей выборке
P(Z)	Априорная вероятность	Базовая распространенность классов в данных $P(Z = k) = \frac{N_k}{N}$, $k \in \{\text{дестр, не дестр}\}$	Доля объектов класса Z в обучающем наборе

Продолжение таблицы 3.9

P(X)	Нормирующая константа	Общая вероятность наблюдения признаков X во всех классах	Сумма P(X|Z)*P(Z) по всем классам

Формула представляет собой байесовский классификатор, который вычисляет вероятность того, что анализируемый контент является деструктивным по классу Z, учитывая все его признаки X.

Таким образом, окончательное решение о принадлежности контента к деструктивному классу является результатом интерпретации апостериорной вероятности.

На рисунке 3.3 представлена схема кросс-модального вероятностного метода классификации.

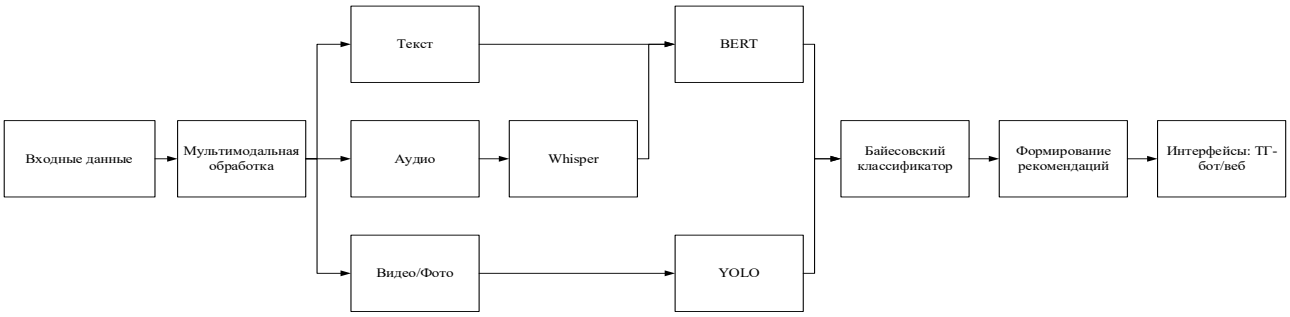


Рисунок 3.3 – Схема кросс-модального вероятностного метода классификации

Вышеописанный метод встраивается в интеллектуальную систему, для формирования решения, например отправка контента на дополнительную проверку модераторам [70]. Для визуализации результатов используются отчеты и рекомендации, которые помогают модераторам принимать обоснованные решения [76-79].

Таким образом, разрабатываемый подход демонстрирует высокую необходимость применения в задачах цифровой обработки аудио, текстовых данных, фото и видео изображений контента.

3.3 Реализация кросс-модального вероятностного метода классификации в корпоративном мессенджере

Встраиваемый в интеллектуальную систему метод позволит повысить точность выявления потенциально деструктивного пользователя [32-34].

Фрагмент кода, демонстрирующий формализацию категорий деструктивного контента, соответствующих таблицам 3.1-3.4 маркеров деструктивности представлен на листинге 3.1.

Листинг 3.1 – Фрагмент кода с примерами категорий деструктивного поведения

```
NEGATIVE_CATEGORIES = [
    'токсичное', 'жалоба', 'деструктивный',
    'экстремизм', 'терроризм', 'насилие', 'буллинг'
]
```

Далее в исследовании продемонстрирован процесс реализации кросс-модального вероятностного метода классификации в корпоративном мессенджере.

Фрагмент кода, демонстрирующий использование моделей NLP и Whisper в вышеописанном методе классификации представлен на листинге 3.2.

Листинг 3.2 – Фрагмент кода использования моделей NLP и Whisper

```
# Загрузка моделей
classifier = MessageClassifier()  # NLP-классификатор
whisper_model = whisper.load_model("base")  # ASR-модель
```

Фрагмент кода, демонстрирующий запуск чат бота для распознавания контекста и обработки мультимодальных данных представлен на листинге 3.3.

Листинг 3.3 – Фрагмент кода запуска чат бота для распознавания контекста и обработки мультимодальных данных

```
if __name__ == '__main__':
    app = ApplicationBuilder().token(TOKEN).build()
    app.add_handler(MessageHandler(filters.TEXT, handle_text_message))
    app.add_handler(MessageHandler(filters.VOICE, handle_voice_message))
    app.add_handler(MessageHandler(filters.VIDEO, handle_video))
    app.run_polling()
```

Фрагмент кода, демонстрирующий формализацию категорий деструктивного контента, соответствующих таблицам маркеров представлен на листинге 3.4.

Листинг 3.4 – Фрагмент кода применения формализации категорий деструктивного контента, соответствующих таблицам маркеров

```
@app.get("/")
def index(request: Request):
    users = SessionLocal().query(User).all()
    summary = []
    for user in users:
        toxic_count = sum(
            1 for msg in user.messages
            if msg.primary_label in NEGATIVE_CATEGORIES  # Анализ по категориям
        )
        summary.append({
            "user_id": user.telegram_id,
            "toxic_count": toxic_count,
            "banned": user.is_banned
        })
    return templates.TemplateResponse(
        "index.html",
        {"request": request, "summary": sorted(summary, key=lambda x: -x["toxic_count"])}
    )
```

На рисунке 3.4 представлен процесс распознавания контекста голосовых сообщений в мессенджере чат ботом.

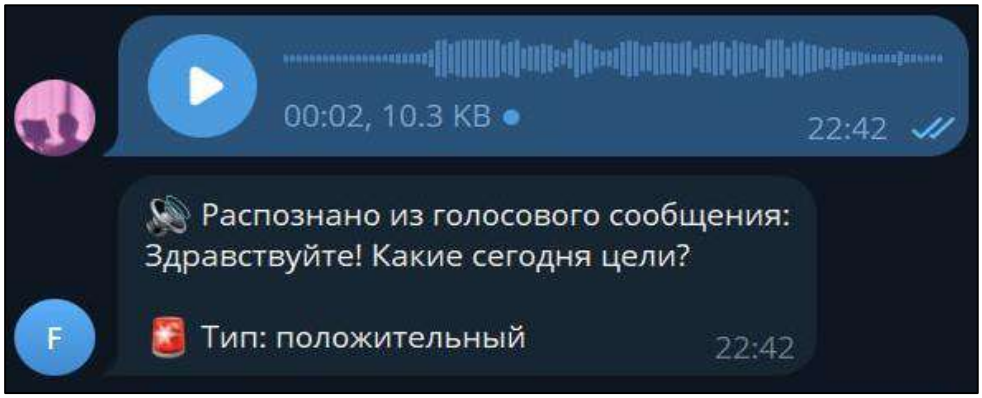


Рисунок 3.4 – Распознавание контекста на примере голосового сообщения

Представленный пример демонстрирует корректное распознавание голосового сообщения в контексте цифровой обработки данных кросс-модального вероятностного метода.

В таблице 3.10 описаны признаки для оценки контекста голосового сообщения пользователя.

Таблица 3.10 – Контекстные признаки для оценки пользователя на примере голосового сообщения

Компонент анализа	**Результат обработки**	**Значение для классификации**
Текстовая расшифровка	«Здравствуйте! Какие сегодня цели?»	Анализ содержания сообщения
Эмоциональная классификация	Тип: положительный	Доброжелательный характер коммуникации

Фрагмент кода, демонстрирующий процесс обработки визуального анализа и аудиоанализа представлен на листинге 3.4.

Листинг 3.5 – Фрагмент кода обработки видео сообщения и распознавание аудио

```
def extract_preview_and_audio(video_path: str):
    clip = mp.VideoFileClip(video_path)
    preview_path = clip.save_frame("preview.jpg", t=0.5)  # Визуальный анализ
    audio_path = clip.audio.write_audiofile("audio.wav")  # Аудиоанализ
    return preview_path, audio_path
```

На рисунке 3.5 продемонстрирован процесс распознавания контекста голосовых и видео сообщений в мессенджере по категории «вопрос».

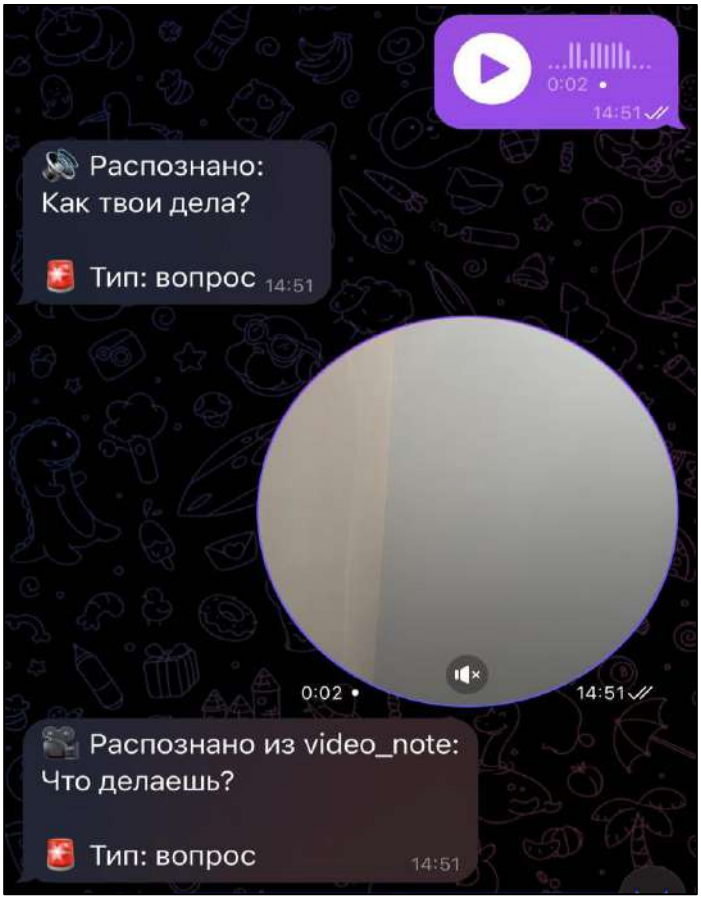


Рисунок 3.5 – Распознавание контекста на примере голосового и видео сообщения по категории «вопрос»

Особенностью представленного примера является корректное определение коммуникативного типа сообщений, несмотря на разницу в каналах передачи информации [67-69].

На рисунке 3.6 продемонстрирован результат обработки видео контента в корпоративном мессенджере.

Видео превью Что делаешь?	**вопрос**	вопрос (0.60), жалоба (0.33), положительный (0.05), деструктивный (0.02), насилие (0.00), буллинг (0.00), экстремизм (0.00), терроризм (0.00)	2025-07-03 11:51:58

Рисунок 3.6 – Результат обработки данных на примере видео сообщений

Результат показывает корректное определение по типу «вопрос» с вероятностью 0.60. Особенно важно отметить, что в проанализированном сообщении были определены возможные скрытые угрозы и их вероятности.

Фрагмент кода, демонстрирующий преобразования аудио сообщения в текст для анализа представлен на листинге 3.6.

Листинг 3.6 – Фрагмент кода преобразования аудио сообщения в текст для анализа

```
async def handle_voice_message(update: Update, context: ContextTypes.DEFAULT_TYPE):
    voice = update.message.voice
    await context.bot.get_file(voice.file_id).download_to_drive("temp.ogg")

    # Этап 1: Аудио->Текст
    AudioSegment.from_ogg("temp.ogg").export("temp.wav", format="wav")
    text = whisper_model.transcribe("temp.wav")["text"]  # Whisper

    # Этап 2: Классификация
    result = classifier.classify_or_flag(text)
    await update.message.reply_text(f"🔊 Тип: {result['primary']}")
```

На рисунке 3.7 продемонстрирован результат обработки аудио сообщений в корпоративном мессенджере.

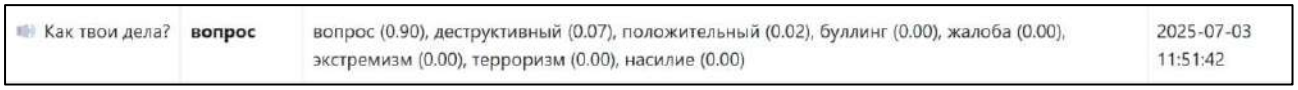


Рисунок 3.7 – Результат обработки данных на примере аудио сообщений

Результат показывает корректное определение по типу «вопрос» с вероятностью 0.90. Особенно важно отметить положительный результат в проанализированном сообщении, несмотря на незначительную вероятность деструктивного подтекста, что подтверждает эффективность байесовского подхода при оценке условных вероятностей различных классов контента.

Фрагмент кода, демонстрирующий обработку текстовых сообщений кросс-модального вероятностного метода классификации представлен на листинге 3.7.

Листинг 3.7 – Фрагмент кода обработки текстовых сообщений кросс-модального вероятностного метода классификации

```
async def handle_text_message(update: Update, context: ContextTypes.DEFAULT_TYPE):
    text = update.message.text
    result = classifier.classify_or_flag(text)  # Этап 1: Классификация
    msg = Message(
        content=text,
        primary_label=result['primary'],  # Результат 1 этапа
        suggestions=json.dumps(result.get('suggestions')),
        user=get_or_create_user(update.effective_user, session)
    )
    session.add(msg)  # Этап 2: Сохранение для байесовского анализа
    await update.message.reply_text(f" Тип: {result['primary']}")
```

Фрагмент кода, демонстрирующий применение байесовского классификатора представлен на листинге 3.8.

Листинг 3.8 – Фрагмент кода применения байесовского классификатора

```
@app.get("/explain/{message_id}")
def explain_message(message_id: int, db: Session = Depends(get_db)):
    message = db.query(Message).filter(Message.id == message_id).first()
    explanation = bayes_explainer.explain(message.content)  # Применение формулы 3.1
    return {
        "message": message.content,
        "explanation": explanation  # Вероятностные оценки
    }
```

На рисунке 3.8 продемонстрирован пример обнаружения новых форм поведения пользователей.

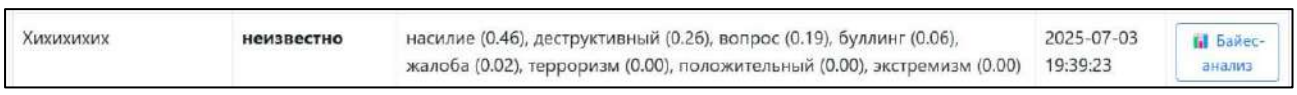


Рисунок 3.8 – Результат обработки данных на примере обнаружения новых форм поведения пользователей

На рисунке представлен пример обработки сообщения «Хихихихих», которое пользователь интерпретировал как выражение смеха, однако кросс-модальный вероятностный метод классификации отнес данный текстовый контент к категории «неизвестно», что активировало механизм обнаружения новых форм деструктивного поведения, класс «Z».

В данном случае высокая оценка потенциально опасного содержания возникла из-за нескольких факторов: необычная орфография, отсутствие четкого семантического значения и возможного контекста общения в корпоративном мессенджере [65, 66].

В контексте данного подхода сохраняется принципиальная важность выявления действительно деструктивных форм поведения, маскирующихся под безобидные на первый взгляд сообщения.

На рисунке 3.9 отображен результат обработки и условная вероятность голосовых сообщений пользователя корпоративного чата.

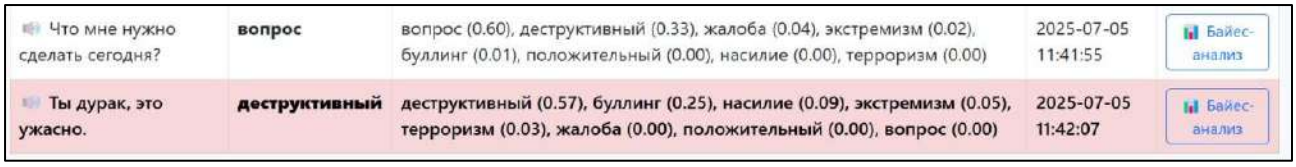


Рисунок 3.9 – Результат обработки данных на примере голосового сообщения одного из пользователей в корпоративном чате

Результат показывает корректное определение по типу «вопрос» с вероятностью 0.60 у первого сообщения и категорию «деструктивный» с вероятностью 0.57 у второго сообщения.

На рисунке 3.10 отображен результат обработки и условная вероятность текстовых сообщений пользователя корпоративного чата.

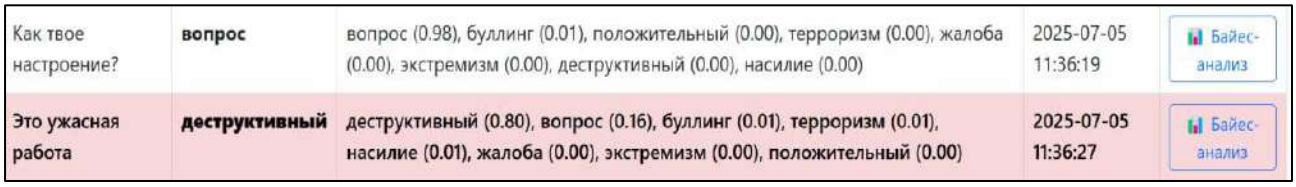


Рисунок 3.10 – Результат обработки данных на примере текстового сообщения одного из пользователей в корпоративном чате

Результат показывает корректное определение по типу «вопрос» с вероятностью 0.98 у первого сообщения и категорию «деструктивный» с вероятностью 0.80 у второго сообщения.

На рисунке 3.11 продемонстрирован результат обнаружения обработки видео сообщения с содержанием жалобы пользователя в корпоративном мессенджере.

Рисунок 3.11 – Результат обработки данных на примере жалобы пользователя в корпоративном чате

На рисунке 3.11 вероятностные оценки демонстрируют сбалансированный подход, где при явном обнаружении категории «жалоба» сохраняется осторожность, учитывая возможность скрытых угроз, присваивая им минимальные вероятности [70].

На рисунке 3.12 представлен фрагмент программного кода из видео сообщения одного из пользователей корпоративного мессенджера, а на рисунке 3.13 отображен результат обработки данного видео сообщения и представлено текстовое распознавание.

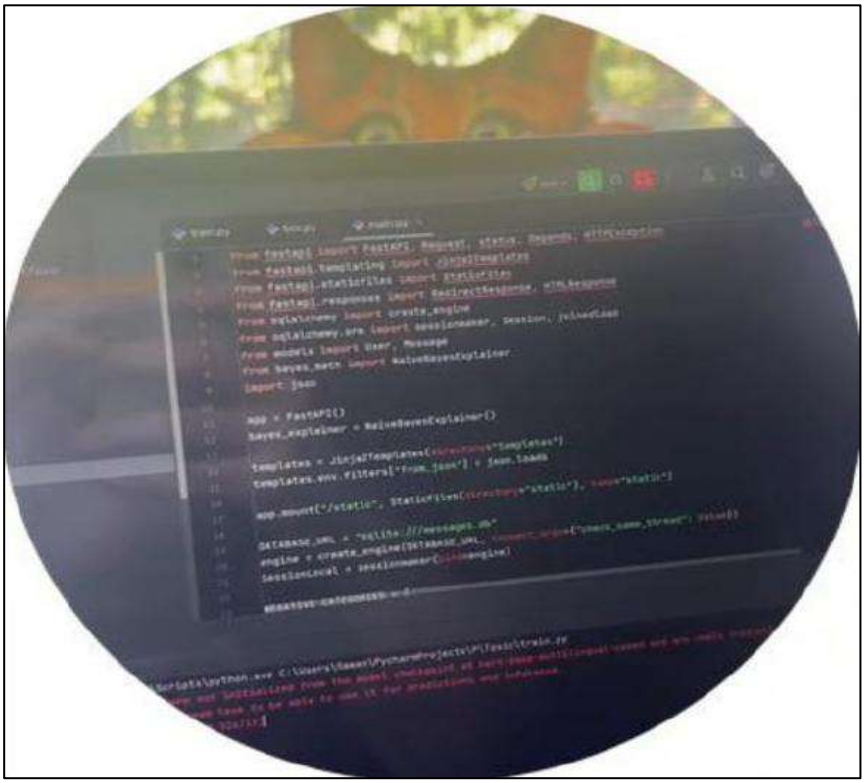


Рисунок 3.12 – Фрагмент программного кода из видео сообщения пользователя

На рисунке 3.13 представлен результат обработки видео сообщения пользователя, содержащего фрагмент программного кода из рисунка 3.12 и распознавание фразы «Я не хочу работать».

Видео превью Я не хочу работать.	**деструктивный**	деструктивный (0.99), буллинг (0.01), жалоба (0.00), насилие (0.00), терроризм (0.00), экстремизм (0.00), положительный (0.00), вопрос (0.00)	2025-07-05 11:46:04	Байес-анализ

Рисунок 3.13 – Результат обработки данных на примере явного обнаружения деструктивного поведения пользователя

На рисунке 3.13 представлен пример обработки данных явного обнаружения деструктивного поведения пользователя в корпоративном мессенджере.

Четкое определение деструктивного характера сообщения с вероятностью 0.99 указывает на потенциальное нарушение трудовой дисциплины.

На рисунке 3.14 продемонстрирована работа Байесовского классификатора.

Рисунок 3.14 – Результат работы Байесовского классификатора

Классификатор рассчитывает итоговую вероятность принадлежности сообщения к каждому классу, используя логарифмические вероятности. Для всех категорий априорная вероятность составляет -2,7515, что соответствует частотности данных классов в обучающей выборке. Наибольшее влияние на итоговый результат оказывает условная вероятность отдельных слов.

Полученные результаты демонстрируют, что классификатор Байеса в контексте двухэтапной классификации эффективно применим для второго этапа подхода.

На рисунке 3.15 продемонстрирована информация о сообщениях на примере одного из пользователей корпоративного мессенджера.

Рисунок 3.15 – Информация о сообщениях на примере одного из пользователей

На представленном рисунке отображена информация по пользователю «424». Сообщение «Привет, как дела?» получило две противоречивые оценки: с одной стороны как положительное с вероятностью 0.72, а с другой высокая вероятность экстремистского содержания с вероятностью 0.70. Данное расхождение в оценках указывает на сложный случай, требующий внимания модератора.

Интерфейс предоставляет возможность блокировки пользователя, оставляя окончательное решение за модератором. Подобные ситуации возникают, когда нейтральные на первый взгляд сообщения содержат скрытые маркеры или рассматриваются в контексте предыдущих действий пользователя.

На рисунке 3.16 представлена информация о пользовательской активности в корпоративном мессенджере.

Рисунок 3.16 – Информация о пользовательской активности на примере одного из пользователей корпоративного мессенджера

На представленном рисунке отображены ключевые метрики одного из пользователей: из 9 отправленных сообщений 2 были классифицированы как токсичные. Текущий статус пользователя сохраняется как «Активен», что указывает на мониторинг пользователей в режиме реального времени, а не автоматическую блокировку.

На рисунке 3.17 представлен отчет о пользовательской активности одного из пользователей корпоративного мессенджера.

Рисунок 3.17 – Отчет о пользовательской активности на примере одного из пользователей корпоративного мессенджера

На рисунке 3.17 анализ сообщений пользователя выявил частые случаи агрессивного поведения, которые были правильно классифицированы как деструктивное поведение с высокими вероятностями. Интерфейс предоставляет модератору возможность блокировки пользователя при сохранении прозрачности принятия решений через отображение всех вероятностных оценок.

На рисунке 3.18 представлен фрагмент интерфейса модератора.

Рисунок 3.18 – Фрагмент интерфейса модератора

На представленном рисунке отображен фрагмент интерфейса модератора, включающий два ключевых функциональных блока. В верхней части экрана расположен инструмент для загрузки CSV-файлов с сообщениями, позволяющий модераторам осуществлять пакетную обработку исторических данных. Ниже отображается сводная таблица активности пользователей, содержащая статистику по пользователям с наиболее высоким уровнем токсичности.

На рисунке 3.19 представлен фрагмент интерфейса о пользовательской активности, отображающий статистику на примере трех учетных записей.

Рисунок 3.19 – Фрагмент интерфейса управления пользователями

На представленном рисунке демонстрируется возможность блокировки пользователей. Интерфейс сохраняет простоту и наглядность, позволяя быстро оценить статус пользователей и при необходимости принять меры.

Фрагмент кода, демонстрирующий блокировку пользователя представлен на листинге 3.9.

Листинг 3.9 – Фрагмент кода блокировка пользователя

```
@app.post("/user/{telegram_id}/ban")
def ban_user(telegram_id: str):
    user = SessionLocal().query(User).filter_by(telegram_id=telegram_id).first()
    if user:
        user.is_banned = True  # Решение на основе анализа
        SessionLocal().commit()
    return RedirectResponse(url=f"/user/{telegram_id}")
```

Разработанный метод с вероятностью 99% идентифицирует сообщение деструктивного поведения, что особенно важно для корпоративных коммуникационных платформ.

Для подтверждения качества кросс-модального вероятностного метода классификации было проведено тестирование в корпоративном мессенджере. В качестве объекта сравнения выбрана действующая система выявления деструктивного поведения в корпоративном мессенджере ООО «АЙТИ КЛАСС».

Расчет показателей проводился на наборе данных объемом 1257 сообщений с экспертной разметкой, что отражено в таблице 3.11.

Таблица 3.11 – Объем набора данных по типу сообщения из корпоративного мессенджера ООО «АЙТИ КЛАСС»

Тип сообщения	**Текстовые сообщения**	**Видео сообщения**	**Фото изображения**	**Аудио сообщения**	**Всего сообщений**
Объем	857	117	194	89	1257

Выражение метрики «точность»:

Для существующего подхода: $\text{Accuracy} = \frac{527+353}{527+353+215+162} = \frac{880}{1257} = 0{,}70$

Для предложенного метода: $\text{Accuracy} = \frac{765+354}{765+354+68+70} = \frac{1119}{1257} = 0{,}89$

Выражение метрики (F1-score):

Для предложенного метода: $\text{Precision} = \frac{765}{765+68} = 0{,}918$

Для предложенного метода: $\text{Recall} = \frac{765}{765+70} = 0{,}916$

Для предложенного метода: $\text{F1} - \text{score} = 2 \times \frac{0{,}918 \times 0{,}916}{0{,}916 + 0{,}918} = 0{,}917$

Существующий подход подразумевал оценку классификации по метрике Recall, численное значение которой составляло 0,60. Для такого значения Recall теоретическое максимальное значение метрики F1-score составляет 0,75 (таблица 3.12).

Результаты демонстрируют, что предложенный метод обеспечивает значительное улучшение по всем ключевым метрикам за счет комплексного анализа мультимодальных данных.

Таблица 3.12 – Результаты сравнения существующего подхода в ООО «АЙТИ КЛАСС» и предложенного кросс-модального вероятностного метода

Критерий	**Существующий подход в ООО «АЙТИ КЛАСС»**	**Предложенный метод**	**Результат**
Точность	70%	89%	+19%
Класс «Z»	60% (*Recall*) (<=0,75 *F1-score*)	92% (*F1-score*)	+>17%

Таким образом, разработанный метод определяет результат, что контент относится к деструктивному поведению пользователя и повышает точность выявления потенциально деструктивного пользователя цифровой платформы.

3.4 Выводы по главе

В третьей главе разработан и детально описан кросс-модальный вероятностный метод классификации текстовых и иных изображений, видео контента. Исследование включает широкий спектр аспектов, обоснование необходимости метода и его этапов, предложив подход, сочетающий анализ мультимодального контента с вероятностными подходами.

Разработанный метод основан на дополнительных признаках классификации со стороны контента и контекста с последующей вероятностной оценкой, что обеспечивает высокую точность выявления деструктивного поведения и его новые формы.

Ключевые результаты, полученные в данной главе:

1. Предложено формализованное описание метода, обеспечивающее точность и воспроизводимость результатов;
2. Этап кросс-модального анализа контента;
3. Этап вероятностной оценки за счет байесовской классификации.

Предложенный метод представляет собой эффективный инструмент для интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде, позволяющий систематизировать процесс выявления новых угроз и повысить точность классификации.

Дальнейшие исследования могут быть направлены на объединение предложенного метода с системами предиктивной аналитики, разработку автоматизированных механизмов обновления классификационных признаков и применения в различных коммуникативных платформах.

ГЛАВА 4. АРХИТЕКТУРА ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАБОТКИ МУЛЬТИМОДАЛЬНЫХ ДАННЫХ В ЦИФРОВОЙ СРЕДЕ

4.1 Обоснование выбора архитектуры интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде

Разрабатываемая архитектура интеллектуальной информационной системы предназначена для анализа поведения пользователей в цифровой среде на основе обработки мультимодальных данных [81-85].

Архитектура интеллектуальной информационной системы обеспечивает высокую производительность, масштабируемость и адаптивность к разнородным данным, включая текст, аудио, видео и изображения [87, 88, 90].

Особенностью цифрового пространства является высокое разнообразие данных, что показывает на необходимость особого подхода к проектированию архитектуры системы [86, 89, 91-93].

В качестве фундаментальных принципов в контексте данного исследования выбраны: адаптивность к различным типам данных, масштабируемость для работы в условиях роста нагрузки и интерпретируемость выводов для модераторов из числа сотрудников.

Способность работать в режиме реального времени является критически важной для оперативного реагирования на выявленные случаи деструктивного поведения [106-108].

Для реализации требований в системе применяется гибридная архитектура, сочетающая преимущества микросервисного и монолитного подходов, конвейерная обработка данных и адаптивные пользовательские интерфейсы. Данное решение позволяет оптимально распределить ресурсы, обеспечивая при этом необходимую гибкость и производительность.

Вышеописанное обоснование архитектуры основывается на комплексе ключевых требований к системе. Для их детализации и структурирования необходим всесторонний анализ.

Таким образом, следующим шагом является анализ требований к интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде.

4.1.1 Анализ требований к архитектуре интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде

Разрабатываемая архитектура интеллектуальной информационной системы предназначена для комплексного анализа поведения пользователей в цифровой среде. На основании исследования были сформулированы ключевые требования к архитектуре системы.

Основным требованием является возможность обработки мультимодальных данных, включая текстовые данные, аудиозаписи, видеоматериалы и изображения, что обусловлено разнородностью цифрового контента на платформах, где информация часто представлена в нескольких взаимодополняющих форматах одновременно [125, 128].

Функциональные требования:

1. Сбор мультимодальных данных из социальных сетей, мессенджеров и коммуникативных платформ;
2. Интеллектуальная обработка данных: текста с использованием Qwen2.5-7B, изображений и видео с использованием YOLO, аудио с использованием Whisper;
3. Реализация двух этапов кросс-модального вероятностного метода классификации контента с выявлением известных и новых (Класс «Z») форм деструктивного поведения;

4. Интеллектуальная группировка пользователей по категориям риска на основе комплексного мультимодального анализа;

5. Формирование структурированных отчетов и понятных рекомендаций для модераторов.

Нефункциональные требования:

1. Производительность: обработка данных в режиме, близком к реальному времени;

2. Масштабируемость: архитектура осуществляет горизонтальное масштабирование модулей;

3. Надежность: отказоустойчивость ключевых компонентов и возможность работы в условиях временного отсутствия связи с источником данных;

4. Безопасность: соответствие требованиям ФЗ-150 «О персональных данных»;

5. Ресурсоэкономность: формирование структурированных и понятных рекомендаций для модераторов.

Критерии выбора архитектуры

1. Возможность подключения к социальным сетям, мессенджерам и цифровым платформам;

2. Оптимизация под ограничительные вычислительные ресурсы организаций;

3. Поддержка модульности для независимого обновления компонентов обработки для разных модальностей;

4. Обеспечение высокой инвариантности моделей к входным данным для минимизации ручной перенастройки.

Далее рассматривается подробное описание компонентов интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде раскрывающее их функциональное назначение и взаимодействие [112, 117].

4.2 Компоненты архитектуры интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде

Архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде включает следующие ключевые модули:

1. Модуль сбора данных;
2. Модуль обработки мультимодальных данных;
3. Модуль кросс-модальной вероятностной классификации;
4. Модуль формирования рекомендаций.

На рисунке 4.1 продемонстрирована диаграмма последовательности формирования рекомендаций в интеллектуальной информационной системе обработки мультимодальных данных.

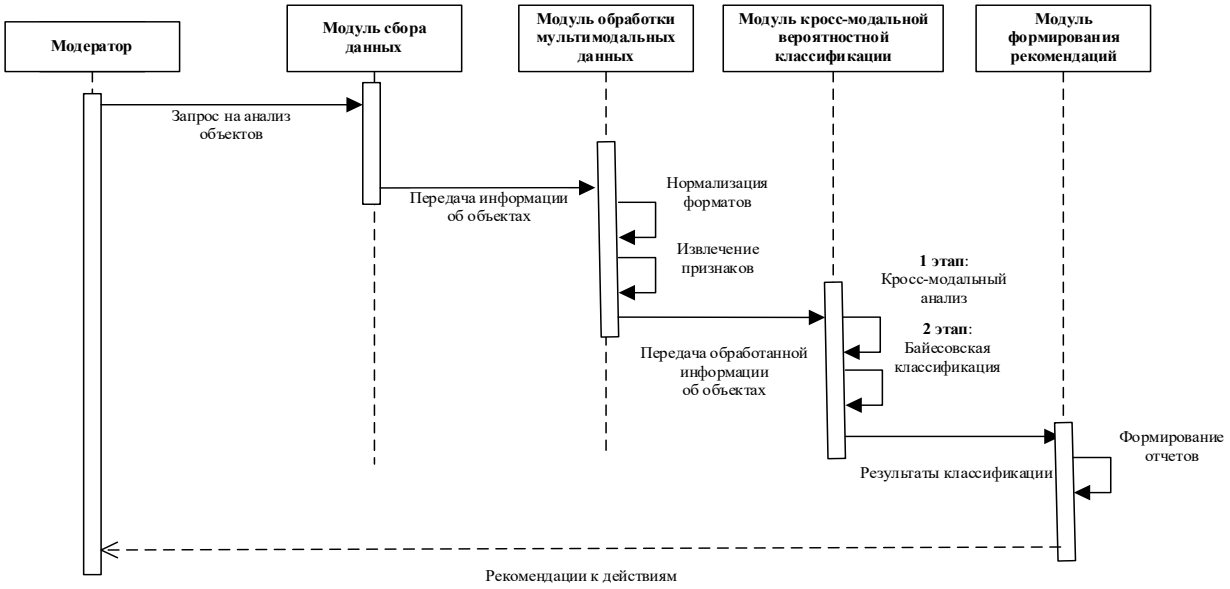


Рисунок 4.1 – Диаграмма последовательности формирования рекомендаций в интеллектуальной информационной системе

Диаграмма описывает процесс взаимодействия компонентов от запроса модератора до формирования рекомендаций.

Далее представлено описание диаграммы:

1. Модератор инициирует процесс, отправляя запрос на анализ объектов, например, текстовых данных, аудио, видео.

2. Модуль сбора данных принимает запрос и передает информацию об объектах, как сырые данные, в модуль обработки мультимодальных данных.

3. Модуль обработки мультимодальных выполняет нормализацию форматов и извлечение признаков, обработанные данные передаются в модуль кросс-модальной вероятностной классификации.

4. Модуль кросс-модальной вероятностной классификации осуществляет на 1 этапе кросс-модального анализа выявление связей между разными типами данных, а на 2 этапе байесовской классификации расчет вероятности деструктивного поведения, включая класс «Z».

5. Модуль формирования рекомендаций создает структурированные результаты анализа в виде отчетов и формирует рекомендации к действиям для модератора.

Представленная диаграмма отражает архитектуру системы, представленную в данной главе, и демонстрирует ее применимость для задач мониторинга в образовательной сфере [12, 14].

На рисунке 4.2 отображена диаграмма развертывания интеллектуальной информационной системы.

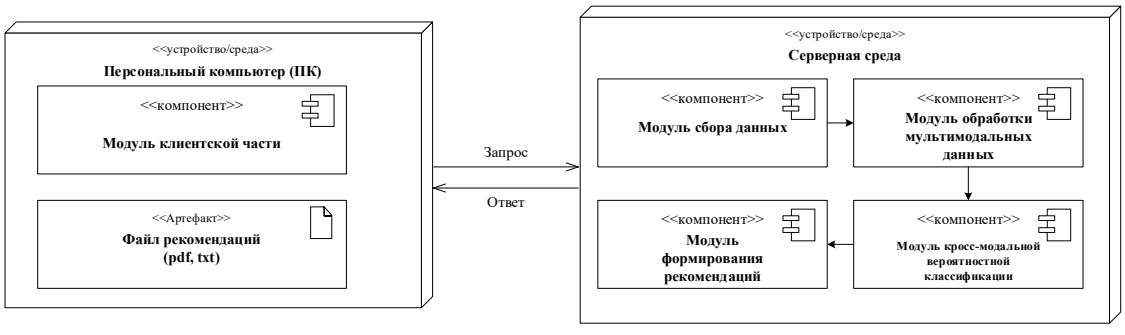


Рисунок 4.2 – Диаграмма развертывания интеллектуальной информационной системы

Диаграмма развертывания отображает архитектуру распределения компонентов системы между физическими устройствами и их взаимодействие, что является важным инструментом размещения частей системы в инфраструктуре и демонстрация обмена данными между ними.

На диаграмме представлено разделение системы на клиентскую и серверную части. Персональный компьютер пользователя-модератора (ПК) выступает в роли клиентского устройства, на котором размещен модуль клиентской части. Данный модуль отвечает за отображение интерфейса для модераторов и получение итоговых файлов с рекомендациями в различных форматах (.pdf, .txt, .xlsx), что обеспечивает гибкость работы с результатами анализа [94-97].

Серверная часть системы включает четыре ключевых компонента, размещенных на сервере. Модуль сбора данных осуществляет мониторинг и сбор контента в различных форматах. Модуль обработки мультимодальных данных обрабатывает разнородный контент для последующего анализа. Модуль кросс-модальной вероятностной классификации осуществляет выявление деструктивного поведения, включая обнаружение новых форм угроз (класс «Z»). Модуль формирования рекомендаций обрабатывает результаты классификации и подготавливает понятные для модераторов выводы [98, 99].

Таким образом, диаграмма представлена в виде четкого разделения функций между клиентской и серверной частями, где сервер осуществляет вычислительную сложную работу по анализу данных, а клиентская часть обеспечивает удобный интерфейс для взаимодействия с системой. Файлы рекомендаций являются артефактами, конкретными результатами работы системы, которые передаются от серверной части к клиентской для использования модераторами [116].

На рисунке 4.3 отображена диаграмма компонентов интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде.

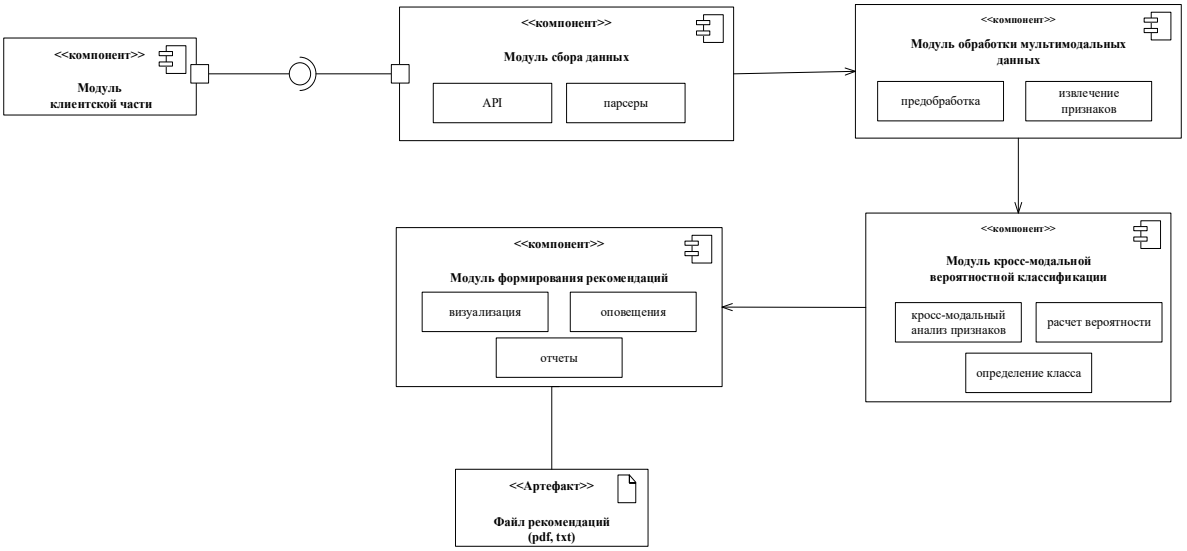


Рисунок 4.3 – Диаграмма компонентов интеллектуальной информационной системы

Диаграмма компонентов отображает основные функциональные модули и их взаимосвязи, что является необходимым инструментом для проектирования архитектуры, позволяя четко определить ответственность каждого элемента системы [11, 13].

Центральными в системе являются модуль обработки мультимодальных данных и модуль кросс-модальной вероятностной классификации, которые выполняют основную аналитическую функцию. Модуль обработки мультимодальных данных получает исходные данные от модуля сбора данных, осуществляющего мониторинг и сбор информации из социальных сетей и мессенджеров. Модуль кросс-модальной вероятностной классификации передает результаты в модуль формирования рекомендаций, для конечного представления результатов в виде отчетов.

Модуль клиентской части обеспечивает интерфейс взаимодействия между системой и модератором. Основная задача данного модуля – предоставление удобного доступа к результатам работы системы, которые оформляются в виде файлов рекомендаций различных форматов. Форматы PDF, TXT и XLSX содержат структурированную информацию о выявленных случаях

деструктивного поведения пользователей и предлагаемых мерах реагирования [110].

На рисунке 4.4 отображена архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде.

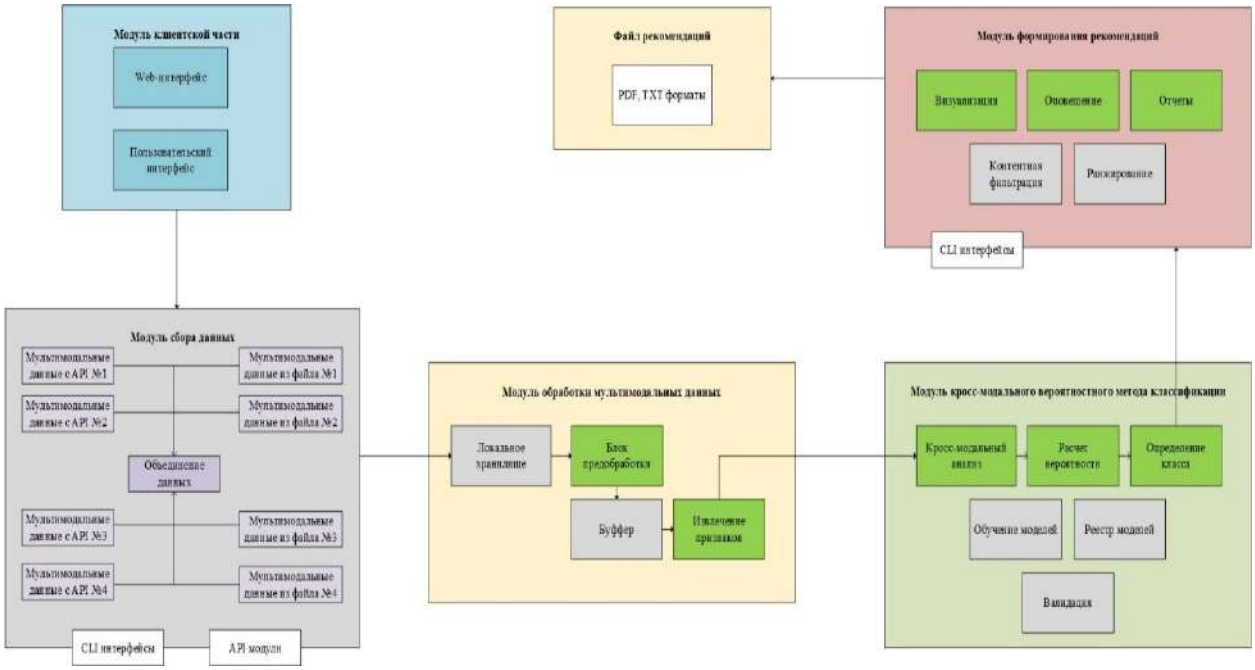


Рисунок 4.4 – Архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде

Архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде демонстрирует принцип однонаправленного потока данных в системе: от сбора данных через последовательные этапы обработки к конечному представлению результатов. Каждый компонент включает определенную функциональность и взаимодействует с другими компонентами через четко определенные интерфейсы, что обеспечивает модульность и легкость сопровождения системы.

Представленная структура компонентов отражает логику работы интеллектуальной информационной системы, где каждый модуль выполняет

строго определенную функцию, а их сочетание обеспечивает комплексный анализ деструктивного поведения в образовательной цифровой среде.

На рисунке 4.5 отображена ИТ-инфраструктура интеллектуальной информационной системы.

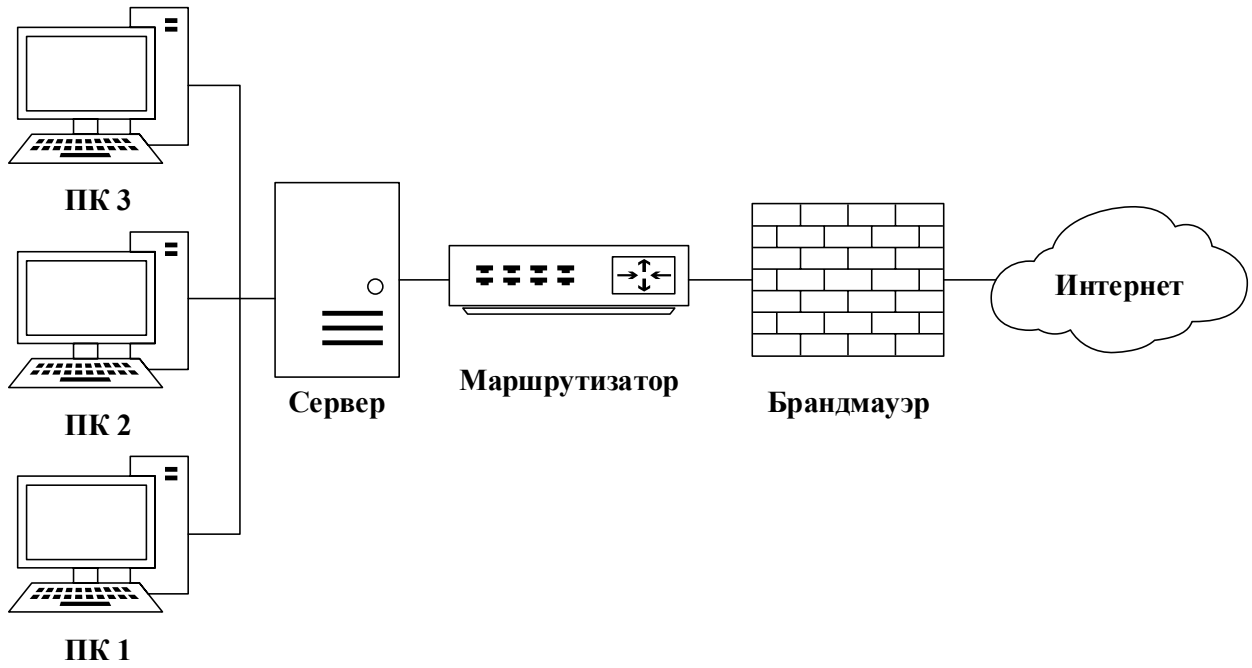


Рисунок 4.5 – ИТ-инфраструктура интеллектуальной информационной системы

В основе ИТ-инфраструктуры лежит централизованная архитектура, где 3 рабочих персональных компьютера (ПК 1, ПК 2, ПК 3) подключены к серверу обработки данных через защищенную сетевую инфраструктуру.

Сервер выполняет ключевую роль в системе, осуществляя интеллектуальную обработку поступающих мультимодальных данных с использованием методов искусственного интеллекта [53]. На сервере реализуется двухэтапная классификация, включающая кросс-модальный анализ и условно-вероятностную оценку. Выбор серверной архитектуры основан на типовых требованиях к аналогичным решениям в образовательной сфере [3-5]. В отличие от крупных центров обработки данных (ЦОД), выбор сервера соответствует реальным условиям образовательных учреждений. Серверная

инфраструктура имеет достаточную производительность для обработки мультимодальных данных исследуемой области, вся информация остается под полным контролем образовательного учреждения, что соответствует требованиям законодательства о защите персональных данных. Система сохраняет базовую функциональность при временных перебоях с интернет-соединением [7, 8]. Архитектура предусматривает возможность постепенного масштабирования при росте нагрузок.

Маршрутизатор в данной ИТ-инфраструктуре выполняет функцию управляющего узла, распределяя информационные потоки между персональными компьютерами и сервером обработки. Маршрутизатор обеспечивает стабильную передачу данных и поддерживает необходимую скорость обработки информации, что особенно важно при работе с большими объемами мультимодального контента в реальном времени [49, 50, 52].

Брандмауэр выступает в качестве защитного барьера системы, обеспечивая фильтрацию входящего и исходящего трафика. Настройки оптимизированы для работы с образовательным контентом.

Для завершения проектирования необходимо перейти к вопросу практической реализации проекта, к описанию динамики их взаимодействия.

4.3 Реализация архитектуры интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде

Практическая реализация архитектуры интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде осуществлялась итеративно, с поэтапным внедрением и тестированием каждого модуля. Для разработки использовался стек технологий, ориентированный на задачи искусственного интеллекта: Python, Qwen2.5-7B, YOLO, Whisper, BERT.

На рисунке 4.6 продемонстрирован бизнес-процесс управления деструктивным поведением в цифровой среде.

Рисунок 4.6 – Бизнес-процесс управления деструктивным поведением в цифровой среде

Мультимодальные данные, поступающие из цифровых платформ, являются входными данными для анализа [80]. На их основе идентифицируется пользователь и его контент, который направляется в интеллектуальную информационную систему для глубокой обработки. На данном этапе реализуется рассмотренный ранее кросс-модальный вероятностной метод классификации.

Результатом являются сформированные рекомендации и потенциальный класс «Z». Модератор, выступая в роли эксперта анализирует полученные выводы и принимает окончательное решение, учитывая как данные системы, так и внешние нормативные требования.

Результаты управления, включая данные о новых угрозах и действия модератора, используются для дообучения моделей интеллектуальной системы.

На рисунке 4.7 представлен единый аналитический контур интеллектуальной информационной системы.

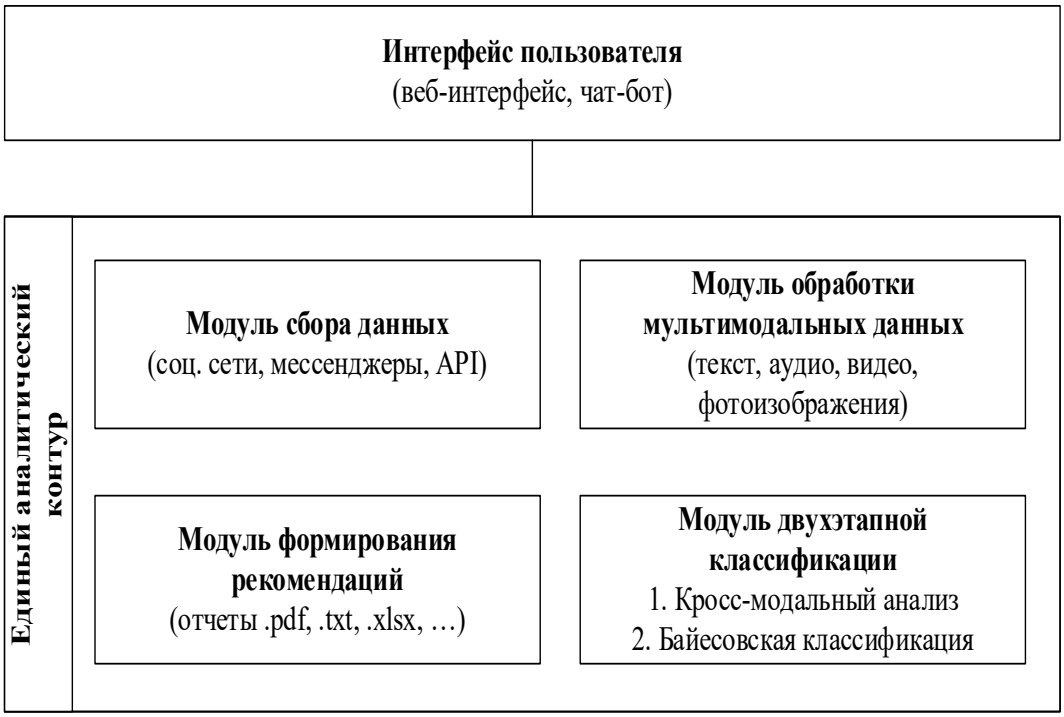


Рисунок 4.7 – Единый аналитический контур интеллектуальной информационной системы

Важной особенностью реализации системы является формирование единого аналитического контура, который включает в себя все этапы обработки данных от сбора мультимодального контента до формирования рекомендаций. Данный контур обеспечивает сквозную согласованность обработки информации и позволяет достичь высокой инвариантности к разнородным данным и адаптивности к новым формам угроз без необходимости ручного вмешательства в систему.

Далее будет рассмотрена схема отражающая последовательность преобразования разнородной информации.

На рисунке 4.8 представлен процесс обработки мультимодальных данных в интеллектуальной информационной системе.

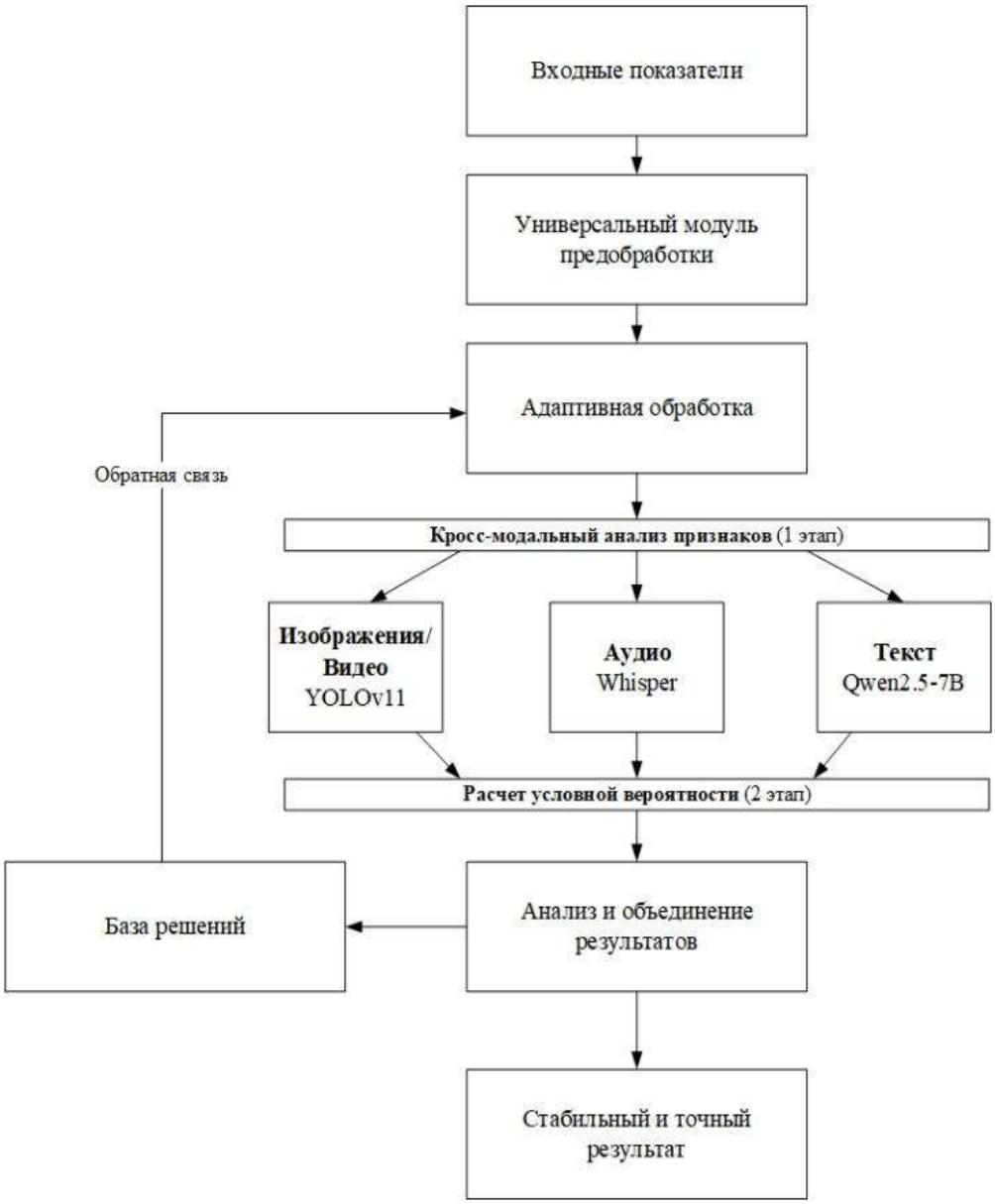


Рисунок 4.8 – Схема процесса обработки мультимодальных данных в интеллектуальной информационной системе

Схема демонстрирует способность системы достичь повышения инвариантности к входным показателям за счет комплекса архитектурных и функциональных решений. Универсальный модуль предобработки выполняет первичную нормализацию разнородных данных, обеспечивая их согласованность на последующих этапах обработки. Специализированные

обработчики для каждого типа данных, основанные на адаптивных моделях искусственного интеллекта, обладают устойчивостью к входным показателям благодаря предобучению.

Ключевым элементом инвариантности является база решений с процессом отправки обратной связи. Данный механизм позволяет системе непрерывно адаптироваться к новым форматам данных и ранее неизвестным типам угроз без необходимой ручной перенастройки моделей. Решения модератора, полученные в результате анализа, сохраняются и используются для дообучения, что расширяет способности системы к автономной обработке изменяющегося контента.

Дополнительное повышение устойчивости достигается за счет кросс-модального анализа, который позволяет взаимно дополнять и корректировать результаты обработки различных типов, что снижает зависимость итоговых результатов от возможных искажений и шумов. Следовательно, система реализует принцип самообучения и адаптации в условиях разнообразия входных данных и изменении цифровых угроз.

На рисунке 4.9 представлена сравнительная схема процесса модерации до и после внедрения интеллектуальной информационной системы.

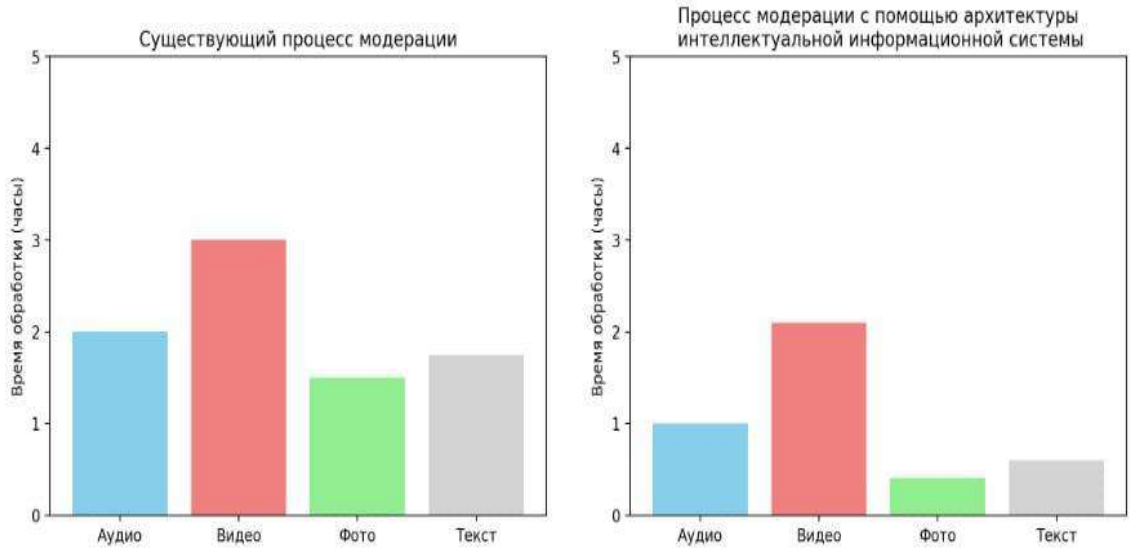


Рисунок 4.9 – Сравнение нагрузки на модератора

На листинге 4.1 представлен процесс построения визуализации сравнения нагрузки на модератора.

Листинг 4.1 – Фрагмент листинга построения визуализации сравнения нагрузки на модератора

```
import streamlit as st
import matplotlib.pyplot as plt
import numpy as np

# 1. Данные
moderator_audio_time = 2  # часов
moderator_video_time = 3  # часов
moderator_photo_time = 1.5  # часов
moderator_text_time = 1.75 # часов
moderator_error_rate = 0.18  # 18% ошибок

ai_audio_time = 1  # часов
ai_video_time = 2.1  # часов
ai_photo_time = 0.4  # часов
ai_text_time = 0.6 # часов
ai_error_rate = 0.055  # 5,5% ошибок

# Определение максимального значения для оси Y (для выравнивания графиков)
max_time = max(moderator_audio_time, moderator_video_time, moderator_photo_time,
moderator_text_time)

    # Столбчатая диаграмма времени обработки
    labels = ['Аудио', 'Видео', 'Фото', 'Текст']  # Добавляем "Текст"
    times = [moderator_audio_time, moderator_video_time, moderator_photo_time,
moderator_text_time]

    # Столбчатая диаграмма времени обработки ИИ
    labels = ['Аудио', 'Видео', 'Фото', 'Текст']  # Добавляем "Текст"
    times = [ai_audio_time, ai_video_time, ai_photo_time, ai_text_time]
```

На рисунке 4.10 представлен процесс модерации до и после внедрения интеллектуальной информационной системы.

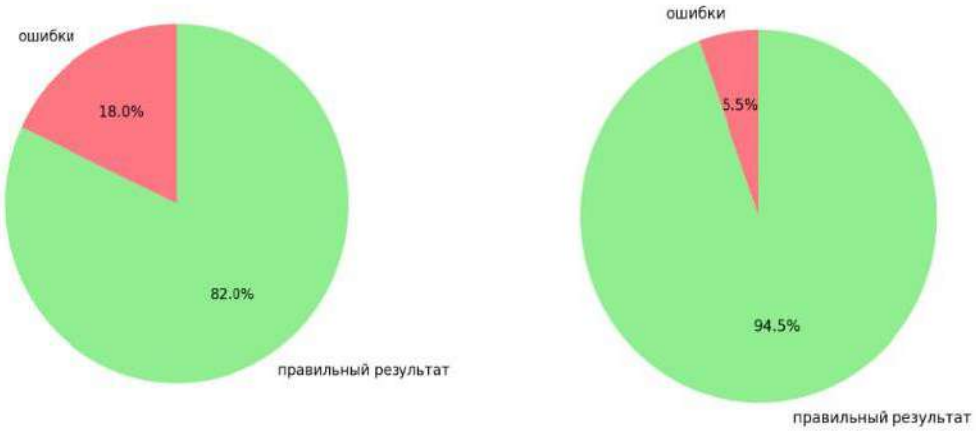


Рисунок 4.10 – Сравнение нагрузки на модератора до и после внедрения интеллектуальной информационной системы

На листинге 4.2 представлен процесс построения визуализации сравнения нагрузки на модератора до и после внедрения интеллектуальной информационной системы.

Листинг 4.2 – Фрагмент листинга построения визуализации сравнения нагрузки на модератора до и после внедрения интеллектуальной информационной системы

```
    # Круговая диаграмма процентов ошибок
    sizes1 = [moderator_error_rate * 100, (1 - moderator_error_rate) * 100]  # Вычисляем
проценты корректно
    labels1 = ["ошибки", "правильный результат"]
    custom_colors1 = ['#FF7782', '#90EE90']

    fig3, ax3 = plt.subplots()  # Создаем новую фигуру и оси для круговой диаграммы
    ax3.pie(sizes1, labels=labels1, autopct='%1.1f%%', startangle=90, colors=custom_colors1)
    ax3.axis('equal')  # Обеспечиваем круглую форму
    st.pyplot(fig3)

# Процент ошибок
    st.subheader(f"Процент ошибок: {moderator_error_rate * 100:.2f}%")

    # Круговая диаграмма процентов ошибок
    sizes2 = [ai_error_rate * 100, (1 - ai_error_rate) * 100]  # Вычисляем проценты
корректно
    labels2 = ["ошибки", "правильный результат"]
    custom_colors2 = ['#FF7782', '#90EE90']
```

Продолжение листинга 4.2

```
fig4, ax4 = plt.subplots()  # Создаем новую фигуру и оси для круговой диаграммы
    ax4.pie(sizes2, labels=labels1, autopct='%1.1f%%', startangle=90, colors=custom_colors2)
    ax4.axis('equal')  # Обеспечиваем круглую форму
    st.pyplot(fig4)

    # Процент ошибок ИИ
    st.subheader(f"Процент ошибок (ИИ): {ai_error_rate * 100:.2f}%")
```

Существующий процесс модерации отображает высокую нагрузку на модератора, где объем данных проверяется вручную.

Разработанная архитектура интеллектуальной информационной системы позволяет обрабатывать 94,5% всего объема данных, сокращая время обработки и освобождая модератора от рутинной работы. Результативность работы возрастает с 82% до 94,5%.

Процесс модерации с помощью архитектуры интеллектуальной информационной системы автоматически выполняет большую часть обработки контента, оставляя модератору наиболее сложные и спорные случаи – 5,5%.

Таким образом, архитектура интеллектуальной информационной системы обеспечивает интерпретируемость выводов для модераторов и адаптивность к различным типам данных, включая текст, аудио, видео и изображения.

В таблице 4.1 представлено комплексное сравнение предложенного решения представленных задач к обработке мультимодальных данных в интеллектуальной информационной системе с существующими подходами.

Таблица 4.1 – Сравнительный анализ подходов к обработке мультимодальных данных в интеллектуальной информационной системе

Задача	**Существующие подходы**	**Предложенное решение**
Обработка разноформатных данных	Разрозненные системы для каждого типа данных, отсутствие единого стандарта обработки	Универсальный модуль предобработки со специализированными искусственными нейронными сетями для каждой модальности

Продолжение таблицы 4.1.

Выявление новых угроз (класс «Z»)	Статические модели с возможностью ручного обновления при появлении угроз	Кросс-модальный вероятностный метод классификации и механизм обратной связи для непрерывного обучения
Энергоэффективность и производительность	Ресурсоемкие алгоритмы, не оптимизированные для работы в условиях ограниченных вычислительных ресурсов	Использование ресурсоэффективных моделей искусственного интеллекта
Инвариантность к входным данным	Обработка конкретных форматов данных, необходимость перенастройки под новые платформы	Адаптивная интеллектуальная обработка разнородных данных

Таким образом, реализованная система на базе предложенной в исследовании архитектуры не просто обрабатывает данные, а адаптируется к ним. Данное свойство инвариантности позволяет стабильно работать с контентом из любых источников.

Реализация архитектуры интеллектуальной информационной системы позволила достичь двух основных показателей: автоматизация рутинных операций, что сокращает нагрузку на модераторов и единый аналитический контур, включающий все этапы обработки.

Данное архитектурное решение обеспечило достижение качественного улучшения показателя инвариантности за счет реализации процесса анализа разнородных данных.

Единый аналитический контур включает все этапы обработки информации от первичного сбора мультимодальных данных до формирования итоговых рекомендаций.

Центральным элементом в контуре выступает модуль кросс-модальной вероятностной классификации осуществляющий кросс-модальный анализ и байесовскую оценку вероятностей. Особенностью контура является получение обратной связи по результатам действий модератора и выявленных форм деструктивного поведения для дообучения моделей.

Реализация единого аналитического контура обеспечивает повышение инвариантности искусственных нейронных сетей к входным показателям. Архитектура интеллектуальной информационной системы демонстрирует качество при обработке контента из различных платформ и в разнородных форматах без необходимости постоянной ручной перенастройки параметров анализа.

В таблице 4.2 представлен сводный анализ результатов эксперимента.

Таблица 4.2 – Сводный анализ результатов эксперимента

Характеристика	**Результат**
Оперативность	Сокращение времени выявления в 125 раз (51000 сообществ и 2000 пользователей
Результативность	Определение деструктивного контента 99%, включая скрытые формы
Ресурсоэкономность	Сокращение трудозатрат модератора за счет автоматизации с 82% до 5,5%
Мультимодальность	Охват всех типов контента и их взаимосвязи (текст, фото, аудио, видео)
Точность	Рост точности на 19% (1257 сообщений в корпоративном мессенджере)
Инвариантность	Устойчивость к изменениям в цифровой среде за счет механизма обратной связи, обработка данных из разных платформ (социальные сети, корпоративные мессенджеры)

Таким образом, описанные этапы проектирования и реализации системы на базе архитектуры позволяют сделать следующие выводы по главе.

4.4 Выводы по главе

В четвертой главе диссертационного исследования была разработана и детально описана архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде, направленная на выявление деструктивного поведения пользователей.

Сбор данных, специализированные искусственные нейронные сети для каждой модальности, кросс-модальная вероятностная классификация и формирование рекомендаций объединены в единый аналитический контур, что обеспечивает целостный и взаимодополняющий анализ цифрового следа пользователя.

Разработанная архитектура интеллектуальной системы является масштабируемой и адаптируемой, что открывает перспективы для ее внедрения в областях, требующих мониторинга и анализа пользовательского поведения в цифровой среде, такие как корпоративная безопасность, управлением репутацией и социальные исследования.

Архитектура интеллектуальной информационной системы демонстрирует качество при обработке контента из различных платформ и в разнородных форматах без необходимости постоянной ручной перенастройки параметров анализа

Представленное решение обеспечивает комплексное повышение эффективности и качества выявления деструктивного поведения в сети Интернет, что проявляется в оперативности, результативности, ресурсоэкономности, мультимодальности, точности и инвариантности.

ЗАКЛЮЧЕНИЕ

В диссертации решена научная задача, состоящая в разработке методов обработки научно-методических и системно-технических средств интеллектуальной системы на основе анализа и цифровой обработки мультимодальных данных, характеризующих деструктивное поведение пользователей в сети Интернет.

Основные результаты проведенного исследования заключаются в следующем:

1. Проведен анализ мультимодальных данных и деструктивного поведения в цифровой среде. Показано, что мультимодальный подход позволяет более точно интерпретировать поведение пользователей, особенно в контексте скрытых угроз.

2. Разработан метод обработки мультимодальных данных из сети Интернет для интеллектуальных систем. В отличие от существующих подходов, метод автоматически формирует новый класс «Z» для потенциально неизвестных (ранее не классифицированных) случаев деструктивного поведения. Разработанный метод сокращает время выявления пользователей, состоящих в деструктивных сообществах в 125 раз, и расширяет мультимодальность исследования цифрового следа за счет комплексного анализа данных из сети Интернет. Практическая значимость метода подтверждена результатами экспериментальных исследований, проведенных на базе РТУ МИРЭА и ООО «НПК «КарбонГрупп» (акты о внедрении результатов диссертационного исследования в приложении диссертации).

3. Разработан кросс-модальный вероятностный метод классификации цифровой обработки аудио, текстовых данных, фото и видеоизображений контента. В отличие от существующих методов, реализуется двухэтапная классификация контента за счет оценки вероятности проявления поведения пользователя, позволяющий определить принадлежность контента к деструктивному и повысить точность выявления потенциально деструктивного

пользователя цифровой платформы на 19%. Практическая значимость подтверждена результатами внедрения в ООО «АЙТИ КЛАСС» (акт о внедрении результатов диссертационного исследования в приложении диссертации).

4. Разработана архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде. В отличие от известных решений, единый аналитический контур включает сбор данных, специализированные искусственные нейронные сети для каждой модальности данных, кросс-модальную вероятностную классификацию и формирование рекомендаций, что позволяет повысить инвариантность к входным показателям без необходимой перенастройки моделей и сократить нагрузку на модераторов интеллектуальной системы (свидетельство о регистрации программы № 2025668422 от 15.07.2025 «Интеллектуальная информационная система обработки мультимодальных данных» и свидетельство о регистрации программы № 2025681455 от 14.08.2025 «Интеллектуальная информационная система обработки данных в образовательной сфере»).

5. Анализ результатов эксперимента всесторонне доказывает, что цель диссертационного исследования достигнута, а поставленные задачи решены. Разработанные методы и архитектура обеспечивают комплексное повышение эффективности и качества выявления деструктивного поведения в сети Интернет, что проявляется в оперативности, результативности, ресурсоэкономности, мультимодальности, точности и инвариантности.

Проведенное исследование вносит значительный вклад в развитие теории и практики интеллектуальной обработки мультимодальных данных из сети Интернет.

Дальнейшие исследования могут быть направлены на масштабирование интеллектуальной системы в рамках предиктивного выявления угроз в коммерческих и образовательных организациях для обеспечения корпоративной безопасности в сети Интернет.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов, К.В. Автоматическое обнаружение гнева и агрессии в речевых сигналах / Т. Н. Балабанова, К. В. Абрамов, А. В. Болдышев, Д. М. Долбин // Экономика. Информатика. – 2023. – Т. 50, № 4. – С. 944-954.

2. Аллакин, В.В. Анализ методов оценки временных рядов сервером мониторинга информационно-телекоммуникационной сети общего пользования / В.В. Аллакин // Техника средств связи. – 2021. – № 2(154). – С. 60-80.

3. Арсентьева, А.Д. Особенности деструктивного контента в социальной сети ВКонтакте / А.Д. Арсентьева // Мониторинг. Образование. Безопасность. – 2023. – Т. 1. – № 1. – С. 36-41.

4. Баженова, Е.А. Форматы медиаконтента исполнительной власти / Е.А. Баженова, С.А. Овчинникова // Язык и речь в Интернете: личность, общество, коммуникация, культура: сборник статей VII Международной научно-практической конференции, Москва, 20 апреля 2023 года. – Москва: Российский университет дружбы народов (РУДН). – 2023. – С. 48-55.

5. Байдулова, Д.Р. Применение машинного обучения в процессе поиска деструктивной информации в web-контенте / Д.Р. Байдулова, В.А. Гостюнина, Н.В. Давидюк // Вопросы информационной безопасности: Материалы III межрегионального вебинара, Саранск-Елец-Астрахань, 21 февраля 2019 года / Составители В.В. Никулин, Н.А. Фортунова. – Саранск-Елец-Астрахань: Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва, 2019. – С. 62-68.

6. Беженцев, А.А. О необходимости внедрения передовых информационных технологий в деятельность субъектов профилактики правонарушений несовершеннолетних / А.А. Беженцев // Региональная информатика "РИ-2010" : Материалы XII Санкт-Петербургской международной конференции, Санкт-Петербург, 20–22 октября 2010 года. – Санкт-Петербург: Федеральное государственное бюджетное учреждение науки Санкт-

Петербургский институт информатики и автоматизации Российской академии наук. – 2010. – С. 154-155.

7. Билых, А.М. Метод и средства для сбора мультимодальных данных с помощью различных нейроинтерфейсов / А.М. Билых, О.В. Наумов // StudNet. – 2022. – Т. 5, № 6. – С. 72.

8. Бормотов, И.В. Модель ценностного мира российской молодежи на основе байесовских интеллектуальных измерений / Р.А. Жуков, С.В. Прокопчина, И.В. Бормотов [и др.] // МИР (Модернизация. Инновации. Развитие). – 2024. – Т. 15, № 1. – С. 96-114.

9. Босенко, Т.М. Интеграция мультимодальных технологий в образовательный процесс на примере разработки модели машинного обучения на платформе Apache Spark // Вестник МГПУ. Серия: Информатика и информатизация образования. – 2025. – № 1(71). – С. 80-89.

10. Булетова, Н.Е. Управление информационными рисками в организации: учебное пособие / Н.Е. Булетова, Н.Н. Карпухина. — Москва: РТУ МИРЭА. – 2024. – 85 с.

11. Бызов, А.А. Интеллектуальный анализ текстов в социальных науках / А.А. Бызов // Социология: методология, методы, математическое моделирование. – 2019. – № 49. – С. 131-160.

12. Виссия, Х.Э. Принятие решений в информационном обществе: учебное пособие / Х.Э. Виссия, В.В. Краснопрошин, А.Н. Вальвачев. – Санкт-Петербург: Лань. – 2022. – С. 216-218.

13. Гвоздев, О.Г. Архитектура автоматизированной информационной системы сопровождения процессов принятия решений по оценке ущерба при отмене крупных международных экономических форумов / О.Г. Гвоздев, М.А. Шахраманьян, А.И. Овсяник // Экономика: вчера, сегодня, завтра. – 2021. – Т. 11. – № 8-1. – С. 310-322.

14. Гехт, А.Б. Гуманитарные проблемы искусственного интеллекта и его применения: монография / А.Б. Гехт, Р.В. Душкин, А.В. Неровный [и др.]. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича. – 2024. – С. 204-212.

15. Голдберг, Д.В. Современные технологии искусственного интеллекта для автоматизации процесса изучения языков / Д.В. Голдберг // Современное профессиональное образование. – 2025. – № 1. – С. 39-42.

16. Горбунова, Ю.П. Классификация деструктивного контента с использованием нейронной сети / Ю.П. Горбунова, О.Ю. Лавлинская // Актуальные проблемы инновационных систем информатизации и безопасности: Материалы международной научно-практической конференции, Воронеж, 26 марта 2025 года. – Воронеж: ООО Издательско-полиграфический центр "Научная книга". – 2025. – С. 60-63.

17. Горбунова, Ю.П. Классификация деструктивного контента с использованием нейронной сети / Ю.П. Горбунова, О.Ю. Лавлинская // Актуальные проблемы инновационных систем информатизации и безопасности: Материалы международной научно-практической конференции, Воронеж, 26 марта 2025 года. – Воронеж: ООО Издательско-полиграфический центр "Научная книга". – 2025. – С. 60-63.

18. Гусев, И.С. Особенности визуального контента в средствах массовой информации и классификация его типов / И.С. Гусев // Неделя науки и творчества - 2024: Материалы Международного научно-практического форума студентов, аспирантов и молодых ученых. В 3-х частях, Санкт-Петербург, 08–13 апреля 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный институт кино и телевидения. – 2024. – С. 60-64.

19. Дунаевская, К.Е. Интернет-мемы как мотиваторы и демотиваторы правового поведения / К.Е. Дунаевская // Молодежный научный потенциал в юриспруденции XXI века: от теории к практике: Сборник статей VI Всероссийской студенческой научно-практической конференции, Москва, 19 октября 2023 года. – Москва: Российский государственный гуманитарный университет. – 2023. – С. 138-148.

20. Дьяченко, Р.А. Обеспечение информационной безопасности вычислительной сети с использованием интеллектуальных систем / В.А. Кучер, А.С. Магомадов, Н.Д. Чигликова, Р.А. Дьяченко // Политематический сетевой

электронный научный журнал Кубанского государственного аграрного университета. – 2015. – № 110. – С. 1811-1816.

21. Енгибарян, М.М. Развитие системы управления персоналом в условиях цифровых трансформаций / М.М. Енгибарян, М.Д. Шалагинова // Молодой исследователь Дона. – 2024. – № 1. – С. 42-48.

22. Епифанцева, К.Г. Применение алгоритмов классификации в системе организации образовательного контента / К.Г. Епифанцева, А.Н. Полетайкин // Обработка информации и математическое моделирование: Материалы Российской научно-технической конференции, Новосибирск, 23–24 апреля 2020 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики. – 2020. – С. 68-72.

23. Ермакова, Л.М. Методы классификации текстов и определения качества контента / Л.М. Ермакова // Вестник Пермского университета. Математика. Механика. Информатика. – 2011. – № 3(7). – С. 47-53.

24. Захаров, С.М. TikTok как средство политизации молодежи: кейс современной России / С.М. Захаров // Известия Иркутского государственного университета. Серия: Политология. Религиоведение. – 2024. – Т. 47. – С. 32-47.

25. Зеленский, А.А. Разработка монитора безопасности от деструктивных влияний веб–сайтов и социальных сетей Интернета / А.А. Зеленский // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: сборник статей VII Всероссийской научно-технической конференции, Таганрог, 05–11 апреля 2021 года. – Таганрог: Южный федеральный университет. – 2021. – С. 29-34.

26. Ибрагимова, Н.И. Опасности в современном мире и методы обучения вопросам безопасности: учебно-методическое пособие / Н.И. Ибрагимова, А.В. Жогаль. – Сургут: СурГУ. – 2024. – С. 20-25.

27. Иванова, Т.В. Психология деструктивного информационно-психологического воздействия: Учебное пособие для студентов, обучающихся по специальности 37.05.02 Психология служебной деятельности / Т. В. Иванова, Ю.М. Тарадина, А.А. Головинский. – Санкт-Петербург: Санкт-Петербургский

университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева. – 2024. – 152 с.

28. Ильгова, Е.В. Функциональная структура автоматизированной информационной системы профилактики безнадзорности и правонарушений несовершеннолетних в Российской Федерации / Е.В. Ильгова, С.Н. Зайкова // Вестник Саратовской государственной юридической академии. – 2021. – № 5(142). – С. 104-113.

29. Исмагулов, М.Е. Современные методы построения мультимодальных систем искусственного интеллекта / М.Е. Исмангулов // Информационные технологии как основа прогрессивных научных исследований: Сборник статей Международной научно-практической конференции, Саратов, 25 июня 2024 года. – Уфа: ООО "Аэтерна". – 2024. – С. 31-35.

30. Ковун, В.А. Применение методов машинного обучения в задачах обеспечения кибербезопасности / В.А. Ковун, И.Л. Каширина // Актуальные проблемы прикладной математики, информатики и механики: сборник трудов Международной научной конференции, Воронеж, 17–19 декабря 2018 года. – Воронеж: Научно-исследовательские публикации. – 2019. – С. 233-239.

31. Козлова, Л.П. Стандартизация в инфокоммуникационных сетях / Л.П. Козлова // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2014): III Международная научно-техническая и научно-методическая конференция: сборник научных статей, Санкт-Петербург, 25–26 февраля 2014 года. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича. – 2014. – С. 475-478.

32. Кольцова, Е.А. Мультимодальный характер цифровой коммуникации: функционирование эмодзи в межличностном общении / Е.А. Кольцова, Ф.И. Карташкова // Вестник Российского университета дружбы

народов. Серия: Теория языка. Семиотика. Семантика. – 2022. – Т. 13, № 3. – С. 769-783.

33. Коротышев, А. П. Манипулятивные технологии в новых медиа: нейросетевые методики и прикладные методы мониторинга / А.П. Коротышев // Манипуляции и социум: язык, сознание, культура: Сборник научных трудов, Калининград, 15–17 мая 2023 года. – Калининград: Балтийский федеральный университет имени Иммануила Канта. – 2023. – С. 218-222.

34. Коротышев, А.П. Метод ПРОЗИС-анализав оценке сетевой активности пользователей / А.П. Коротышев // Возможности и угрозы цифрового общества: материалы Всероссийской научно-практической конференции, Ярославль, 20–22 апреля 2023 года. – Ярославль: Общество с ограниченной ответственностью "Филигрань". – 2023. – С. 222-235.

35. Коротышев, А.П. Цифровые коммуникативные практики: нейросетевые и математические модели, возможности прикладного анализа / А.П. Коротышев // Коммуникативные практики современной молодежи: перспективы и вызовы: Материалы Международной научно-практической конференции, Нижний Новгород, 15–16 сентября 2022 года. – Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского. – 2022. – С. 464-469.

36. Кучук, Е.А. Прогнозирование конфликтов с использованием методов Data Science и сетевого анализа / Е.А. Кучук // Аналитические технологии в социальной сфере: теория и практика, Москва, 14 декабря 2023 года. Том Выпуск 15. – Москва: Изд-во НИЦ «Национальная безопасность». – 2023. – С. 44-49.

37. Леоненко, С.С. Защита интеллектуальной собственности в цифровой среде / С.С. Леоненко, А.А. Елизарова // Вестник Ивановского государственного университета. Серия: Естественные, общественные науки. – 2025. – № 1. – С. 94-104.

38. Гришков, А.К. Метод предварительной обработки информации в интеллектуальных системах распознавания и ввода данных / А.К. Гришко, А.В.

Моисеев, А.А. Пакайкин [и др.] // Инновационные, информационные и коммуникационные технологии : сборник трудов XVII Международной научно-практической конференции, Сочи, 01–10 октября 2020 года / под.ред. С.У.Увайсов. – Москва: Ассоциация выпускников и сотрудников ВВИА имени профессора Н.Е.Жуковского содействия сохранению исторического и научного наследия ВВИА имени профессора Н.Е. Жуковского. – 2020. – С. 351-353.

39. Миллер, Д.Д. Обзор методов интеллектуального анализадля прогнозирования освоения массового открытого онлайн-курса / Д.Д. Миллер // Цифровые технологии в образовании, науке, обществе: Материалы XV Всероссийской научно-практической конференции, Петрозаводск, 30 ноября – 03 декабря 2021 года. – Петрозаводск: Петрозаводский государственный университет. – 2021. – С. 78-80.

40. Минаев, В.А. Результаты компьютерных экспериментов по идентификации деструктивного контента в социальных медиа / В.А. Минаев, К.М. Бондарь // Актуальные проблемы науки и практики: Сборник научных трудов по итогам научно-представительских мероприятий, Хабаровск, 23 июня – 01 июля 2022 года. – Хабаровск: Дальневосточный юридический институт Министерства внутренних дел Российской Федерации. – 2022. – С. 46-52.

41. Михненко, П.А. «Анализ мультимодальных данных в управлении проектами: перспективы использования машинного обучения» / П.А. Михненко // Управленческие науки. – Т. 13. – № 4. – 2023. – С. 71-89.

42. Михненко, П.А. Мультимодальная бизнес-аналитика: концепция и перспективы использования в экономической науке и практике / П.А. Михненко // Управленец. Т. 14. – № 6. – 2023. – С. 2–18.

43. Морозов, С.О. Программная реализация информационной системы анализа данных электронной эксплуатационной документации / С.О. Морозов // Перспективы науки. – 2023. – № 8(167). – С. 45-48.

44. Москвитин, А.А. Данные, информация, знания: методология, теория, технологии: монография / А.А. Москвитин // Санкт-Петербург: Лань. – 2022. – С. 171-174.

45. Науразова, Э.А. Информационно-логические инварианты и их приложения / Э.А. Науразова, С.Р. Шамилев // Электронный мультидисциплинарный научный журнал с порталом международных научно-практических конференций Интернетнаука. – 2016. – № 8. – С. 33-40.

46. Нелюбина, Ю.А. Обобщенная архитектура программной системы обработки темпоральных мультимодальных данных цифровых двойников / Ю.А. Нелюбина, В.Н. Тимохин // Инструменты проектного управления и анализа данных в системах поддержки принятия решений: Сборник материалов V Всероссийской Международной конференции, Донецк, 18 апреля 2024 года. – Донецк - Екатеринбург: Донецкий национальный технический университет. – 2024. – С. 72-77.

47. Никифоров, А.А. Разработка архитектуры интеллектуальной информационной системы разработки и анализа данных документации с поддержкой принятия решения / А.А. Никифоров, Д.Е. Гармышев, И.А. Важенин, Н.Г. Левченко // Транспортное дело России. – 2021. – № 2. – С. 96-100.

48. Никулина, И.В. Психология кадровой безопасности: учебное пособие. – Самара: Самарский университет. – 2021. – 80 с.

49. Олешкова, А.М. Интернет-мем как предмет социологического исследования: возможности применения метода событийного анализа (event-analysis) / А.М. Олешкова // Общество: социология, психология, педагогика. – 2020. – № 10(78). – С. 54-57.

50. Онтужева, Г.А. Моделирование системы управления ресурсами гетерогенной распределенной системы обработки информации на основе мультиагентного подхода / Г.А. Онтужева, О.А. Антамошкин // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. – 2016. – Т. 17, № 3. – С. 602-610.

51. Панкратова, М.Д. Модели NLP с использованием нейронных сетей в анализе тональности новостей / М.Д. Панкратова, Т.Н. Сковпень // Аналитические технологии в социальной сфере: теория и практика, Москва, 14

декабря 2023 года. Том Выпуск 15. – Москва: Изд-во НИЦ «Национальная безопасность». – 2023. – С. 97-107.

52. Патент № 2402885 C2 Российская Федерация, МПК H04N 7/26, G06T 7/00. Классификация контента для обработки мультимедийных данных: № 2007137462/09: заявл. 10.03.2006: опубл. 27.10.2010 / В.Р. Равииндран, П. Бхамидипади, Г.К. Уолкер.

53. Патент № 2696345 C2 Российская Федерация, МПК A63F 13/60. Интеллектуальное потоковое воспроизведение мультимедийного контента: № 2017108527: заявл. 14.09.2015: опубл. 01.08.2019 / Д.Р. Джастис, Ю.П. Гарден; заявитель МАЙКРОСОФТ ТЕКНОЛОДЖИ ЛАЙСЕНСИНГ, ЭлЭлСи.

54. Перцев, Ю.В. Методы анализа текста на естественном языке в задаче экстрактивного информационного поиска / Ю.В. Перцев // Успехи кибернетики. – 2024. – Т. 5, № 4. – С. 67-74.

55. Пильгун, М.А. Когнитивная модель анализа контента цифровых коммуникаций / М.А. Пильгун // Вопросы психолингвистики. – 2023. – № 2(56). – С. 68-93.

56. Плуженская, Л.В. Сторителлинг как коммуникативная стратегия образовательных технологий / Л.В. Плуженская // Актуальные вопросы теории и методики профессионального образования: Материалы научно-практической конференции, Ярославль, 19–21 марта 2024 года. – Ярославль: РИО ЯГПУ. – 2024. – С. 121-127.

57. Попов, Г.А. О концепции создания интеллектуальных систем защиты информации на основе нейросетевых систем обнаружения вторжений в АСОД / С.Ж. Симаворян, А.Р. Симонян, Е.И. Улитина, Г.А. Попов // Программные системы и вычислительные методы. – 2019. – № 3. – С. 30-36.

58. Попова, О.А. Перспективы использования искусственного интеллекта в целях обеспечения информационной безопасности граждан от деструктивного контента и фейков / О.А. Попова // Российское общество и социально-правовые аспекты его безопасности: Сборник материалов Всероссийской научно-практической конференции с международным участием,

Москва, 25–26 апреля 2024 года. – Москва: Университет прокуратуры РФ. – 2024. – С. 163-169.

59. Путинцева, А.В. Механизмы защиты личности от кибербуллинга в Российской Федерации / А.В. Путинцева // Вопросы российского и международного права. – 2020. – Том 10. – № 6А. – С. 108-115.

60. Радионцева, Е.С. Информационные поводы: технологии выхода компаний в медиапространство / Е.С. Радионцева // Коммуникативные исследования. – 2023. – Т. 10. – № 2. – С. 317-333.

61. Ренжигло, Р.Е. влияние деструктивного интернет-контента на формирование экстремистских взглядов у молодежи / Р.Е. Ренжигло // Вестник Донецкого национального университета. Серия Е: Юридические науки. – 2023. – № 2. – С. 43-50.

62. Рожков, А.П. Модель интеллектуальной информационной системы, основанной на экспертном знании и углубленной обработке данных о проблемной области / А.П. Рожков, Ф.Ф. Иванов // Север России: стратегии и перспективы развития: Материалы III Всероссийской научно-практической конференции. В 3-х томах, Сургут, 26 мая 2017 года. Том II. – Сургут: Сургутский государственный университет. – 2017. – С. 136-140.

63. Рыбакова, А.С. Уголовно-правовое противодействие распространению деструктивного контента в виде треш-стримов / А. С. Рыбакова // Правовой классицизм и постмодерн в праве традиции и новации: Материалы Всероссийской научно-практической конференции, Иркутск, 26 октября 2024 года. – Иркутск: Издательство ИГУ. – 2024. – С. 138-140.

64. Рыхтик, П.П. ПРОЗИС-анализ: возможности оценки реакции пользователей на значимые информационные поводы в сети Интернет / Р.В. Голубин, И.А. Исакова, А.П. Коротышев, П.П. Рыхтик // Вестник Томского государственного университета. – 2022. – № 475. – С. 59-67.

65. Рябчиков, И.А. Метод автоматического распознавания девиантного поведения людей на основе интеграции технологий компьютерного зрения и управления знаниями для поддержки принятия решений операторами систем

видеомониторинга / И.А. Рябчиков // Системы анализа и обработки данных. – 2022. – № 3(87). – С. 21-36.

66. Савенко, А.Г. Использование интеллектуальной цифровой платформы в образовательном процессе / А.Г. Савенко, А.И. Парамонов // Прикладной искусственный интеллект: перспективы и риски: Сборник докладов Международной научной конференции, Санкт-Петербург, 17 октября 2024 года. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения. – 2024. – С. 166-168.

67. Савищенко, Д.Н. Риск-анализ контента социальных сетей на основе нейросетевой классификации эмоциональной окраски текста сообщений / К.А. Разинкин, Е.С. Соколова, Д.Н. Савищенко, Е.Ю. Чапурин // Моделирование, оптимизация и информационные технологии. – 2021. – Т. 9, № 4(35).

68. Салып, Б.Ю. Анализ модели BERT как инструмента определения меры смысловой близости предложений естественного языка / Б.Ю. Салып, А.А. Смирнов // StudNet. – 2022. – Т. 5, № 5. – С. 33.

69. Свидетельство о государственной регистрации программы для ЭВМ № 2025668422 Российская Федерация. «Интеллектуальная информационная система обработки мультимодальных данных»: заявл. 04.07.2025: опубл. 15.07.2025 / Н. Н. Тетерин.

70. Свидетельство о государственной регистрации программы для ЭВМ 2025681455 Российская Федерация. «Интеллектуальная информационная система обработки данных в образовательной сфере»: заявл. 04.07.2025: опубл. 14.08.2025 / Н. Н. Тетерин.

71. Свидетельство о государственной регистрации программы для ЭВМ № 2025683295 Российская Федерация. Программная реализация классификации текстовых данных: заявл. 20.08.2025: опубл. 02.09.2025 / Н.Н. Тетерин.

72. Свидетельство о государственной регистрации программы для ЭВМ № 2025687164 Российская Федерация. Программная реализация метода

двухэтапной классификации контента: заявл. 24.09.2025: опубл. 08.10.2025 / Н.Н. Тетерин.

73. Свидетельство о государственной регистрации программы для ЭВМ № 2023611498 Российская Федерация. Прототип интеллектуальной платформы для автоматизированной адаптации видео- и аудио- контента на разные языки: № 2022686329: заявл. 27.12.2022: опубл. 20.01.2023; заявитель Общество с ограниченной ответственностью "ДАБ ДАБ".

74. Сенцов, Ф. А. Анализ потенциально-опасного контента в социальной сети "Telegram" / Ф. А. Сенцов, М. В. Янаева // Международный журнал гуманитарных и естественных наук. – 2022. – № 8-2(71). – С. 60-62.

75. Серова, А. И. Использование методов машинного обучения для определения нарушений целостности JPEG-изображений / А. И. Серова, А. И. Спивак // Научно-технический вестник информационных технологий, механики и оптики. – 2018. – Т. 18, № 2. – С. 299-306.

76. Симонян, А.Р. Анализ возможностей адаптации общей схемы иммунной системы в системах противодействия вторжениям / С.Ж. Симаворян, А.Р. Симонян, Г.А. Попов, Е.И. Улитина // Вопросы безопасности. – 2020. – № 4. – С. 36-46.

77. Скрипкина, Т. П. Анализ деструктивного информационно-психологического воздействия посредством телекоммуникационных технологий на российских пользователей / Т. П. Скрипкина, А. А. Макаренков // Вестник Московского государственного областного университета. – 2022. – № 4.

78. Старусев, А.В. Анализ информационных потоков во фрагменте интеллектуальной системы / А.В. Старусев, Л.А. Михолап, Н.Г. Мустафаев, С.П. Литвинов // Стратегия научно-технологического развития россии: проблемы и перспективы реализации: сборник статей Международной научно-практической конференции, Петрозаводск, 12 апреля 2020 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука». – 2020. – С. 39-43.

79. Тарасова, А.В. Методика оценки деловой репутации и ее роль в оптимизации бизнес-процессов // Регион: системы, экономика, управление. – 2021. – № 4. – С. 161-168.

80. Тетерин, Н.Н. Концепция архитектуры информационной системы выявления деструктивного поведения в организационных системах // System Analysis & Mathematical Modeling. – 2025. – Т. 7, № 2. – С. 204–213.

81. Тетерин, Н.Н. Методика обработки и интеллектуальной группировки мультимодальных данных // Научно-аналитический журнал "Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России". – 2025. – №3. – С. 188-194.

82. Тетерин, Н.Н. / Разработка архитектуры интеллектуальной информационной системы обработки мультимодальных данных в цифровой образовательной среде // Экономика и качество систем связи. – 2025. – № 3(37). – С. 158-169.

83. Тетерин, Н.Н. Влияние новой информационной системы на управление организационными системами / Н.Н. Тетерин, Ю.В. Чебернова // Конкурентоспособность в глобальном мире: экономика, наука, технологии. – 2023. – № 6. – С. 71-72.

84. Тетерин, Н.Н. К вопросу выявления деструктивного поведения на основе анализа текстовых данных с использованием методов машинного обучения / Н.Н. Тетерин, В.В. Смоленцева // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2025. – № 4/2. – С. 126-129.

85. Тетерин, Н.Н. К вопросу формализации задачи выявления деструктивного поведения с применением технологий искусственного интеллекта / Н.Н. Тетерин, В.В. Смоленцева // Тенденции развития науки и образования. – 2024. – № 114-10. – С. 81-83.

86. Тетерин, Н.Н. Кросс-модальный вероятностный метод классификации цифровой обработки мультимодальных данных / Н.Н. Тетерин,

Т.Е. Саратова // Безопасность. Управление. Искусственный интеллект. – 2025. – № 4. – С. 9-13.

87. Тетерин, Н.Н. Комплексный подход к разработке методических и алгоритмических средств поддержки принятия решений в управлении деструктивным поведением интернет-пользователей / Н.Н. Тетерин // Техника и безопасность объектов уголовно-исполнительной системы: Сборник материалов Международной научно-практической конференции. В 4-х томах, Воронеж, 14–15 мая 2025 года. – Воронеж: ИП Копыльцов П.И., 2025. – С. 573-575.

88. Тетерин, Н.Н. Концептуальный подход классификации деструктивного поведения с применением технологий искусственного интеллекта / Н.Н. Тетерин, В.В. Смоленцева // Актуальные проблемы прикладной математики, информатики и механики: Сборник трудов Международной научной конференции, Воронеж, 02–04 декабря 2024 года. – Воронеж: Научно-исследовательские публикации. – 2025. – С. 326-329.

89. Тетерин, Н.Н. Обработка данных из сети Интернет для интеллектуальных систем / Тетерин Н.Н, Климкин Е.В. // Современные достижения технических наук: новые горизонты знаний, нанотехнологии: Сборник научных статей – 2025. – С. 35-38.

90. Тетерин, Н.Н. Обработка и аннотирование данных в распределенной системе интеллектуального анализа видеопотоков для детекции деструктивного поведения. / Н.Н. Тетерин, Т.Е. Смоленцева // Computational Nanotechnology. – 2025. – Т. 12. – №3. – С. 79-86.

91. Тетерин, Н.Н. Общие вопросы анализа деструктивного поведения пользователей в социальных сетях // Актуальные проблемы деятельности подразделений уголовно-исполнительной системы: Сборник материалов Всероссийской научно-практической конференции. В 3-х томах, Воронеж, 24 октября 2024 года. – Воронеж: ООО Издательско-полиграфический центр "Научная книга". – 2024. – С. 96-99.

92. Тимохин, А.В. Интеллектуальные технологии в системах управления образовательным контентом на цифровых платформах / А.В. Тимохин, С.В. Рындина // Вестник Пензенского государственного университета. – 2022. – № 3(39). – С. 76-80.

93. Тоичкин Н.А. Проектирование архитектуры информационной системы диагностики состояний и управления безопасностью технологических процессов / Н.А. Тоичкин // Научно-технический вестник Поволжья. – 2023. – № 3. – С. 128-132.

94. Толстых, М.Ю. Приложение-детектор деструктивного контента в музыкальных произведениях Arfa / М.Ю. Толстых, М.В. Баханов // Математические методы и информационно-технические средства: Материалы XX Международной научно-практической конференции, Краснодар, 06 июня 2024 года. – Краснодар: Краснодарский университет МВД РФ. – 2024. – С. 292-296.

95. Углова, А.Б. Анализ деструктивного контента телеграмм-каналов как фактора развития саморазрушающего поведения / А.Б. Углова, Б.А. Низомутдинов // International Journal of Open Information Technologies. – 2022. – Vol. 10. – No. 11.

96. Уздяев, М.Ю. Создание и анализ многомодального корпуса данных для автоматического распознавания агрессивного поведения людей / М.Ю. Уздяев, А.А. Карпов // Научно-технический вестник информационных технологий, механики и оптики. – 2024. – Т. 24. – № 5. – С. 834-842.

97. Фраленко, В.П. Автоматическая классификация изображений в задачах фильтрации контента / В.П. Фраленко, Р.Е. Суворов, Р.И. Овчаренко, И.А. Тихомиров // Информационные технологии и вычислительные системы. – 2015. – № 3. – С. 3-11.

98. Фролов, Д.О. Применение нейросетевых моделей для поиска в мультимодальных данных / Д.О. Фролов, А.Н. Петрова // Молодёжь и наука: актуальные проблемы фундаментальных и прикладных исследований: Материалы VIII Всероссийской национальной научной конференции молодых

учёных, Комсомольск-на-Амуре, 07–11 апреля 2025 года. – Комсомольск-на-Амуре: Комсомольский-на-Амуре государственный университет. – 2025. – С. 565-568.

99. Фролов, Д.О. Разработка нейронных сетей для сквозного обучения моделей поиска информации / А.Н. Петрова, Д.О. Фролов // Ученые записки Комсомольского-на-Амуре государственного технического университета. – 2024. – № 3(75). – С. 48-52.

100. Царькова, Е.Г. О возможности распознавания системой интеллектуального видеонаблюдения девиантного поведения лиц на территории охраняемых объектов УИС / Е.Г. Царькова // Пенитенциарная безопасность: национальные традиции и зарубежный опыт: Материалы Всероссийской научно-практической конференции с международным участием, Самара, 01–02 июня 2023 года. – Самара: Самарский юридический институт ФСИН России. – 2023. – С. 210-212.

101. Черкасова, И.С. Классификация видео контента на основе сверточных нейронных сетей / И.С. Черкасова // E-Scio. – 2021. – № 12(63). – С. 395-405.

102. Черкесова, Л.В. Анализ возможных решений противодействия деструктивному контенту / Л.В. Черкесова, А.И. Ревякин, Е.А. Ревякина // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2021. – № 2. – С. 95-98.

103. Чудинов, С.И. Когнитивная и информационно-психологическая уязвимость студенческой молодежи по отношению к деструктивному контенту / С.И. Чудинов // Обзор.НЦПТИ. – 2024. – № 4(39). – С. 70-78.

104. Шевченко, Д.А. Актуальные аспекты воздействия различных информационных источников на деструктивное поведение молодежи / Д.А. Шевченко // Актуальные вопросы юридической науки глазами молодых исследователей: Сборник статей по итогам Четвертой Всероссийской научной конференции курсантов, студентов, адъюнктов, аспирантов и соискателей, Рязань, 02 февраля 2024 года. – Москва - Нижний Новгород: Постер-М,

Российская академия народного хозяйства и государственной службы при Президенте РФ. – 2024. – С. 155-158.

105. Широких, И.В. Специфика текста как продукта искусственного интеллекта / И.В. Широких, А.Г. Фомин // Искусственный интеллект в автоматизированных системах управления и обработки данных: Сборник статей II Всероссийской научной конференции: в 5 томах, Москва, 27–28 апреля 2023 года. – Москва: КДУ, Добросвет. – 2023. – С. 349-355.

106. Эргешова, А.Ж. Роль искусственного интеллекта в профилактике деструктивного поведения среди молодежи / А.Ж. Эргешова // Актуальные тенденции социальных коммуникаций: история и современность: Сборник научных статей. – Ижевск: Издательский дом "Удмуртский университет". – 2024. – С. 439-442.

107. Applications of machine learning in real-time control systems: a review / X. Zhao, Y. Sun, Ya. Li [et al.] // Measurement Science and Technology. – 2025. – Vol. 36, No. 1. – P. 012003.

108. A commentary on ‘Toxicities associated with immune checkpoint inhibitors: a systematic study’ / G. Lin, Xu. Sun, K. Kang [et al.] // International Journal of Surgery. – 2024.

109. Application of intelligent decision support system for processing a big data of heterogeneous information / S. M. Makeev, I. V. Belikov, I. V. Lebedev, V. I. Perov // Modern informatization problems in the technological and telecommunication systems analysis and synthesis (MIP-2020'AS): Proceedings of the XXV-th International Open Science Conference, Yelm, WA, USA, 10 января 2020 года. – Yelm, WA, USA: Science Book Publishing House LLC, 2020. – P. 247-251.

110. Association of Arterial Metabolic Content with Cerebral Blood Flow Regulation and Cerebral Energy Metabolism–A Multimodality Analysis in Aneurysmal Subarachnoid Hemorrhage / T. Svedung Wettervik, A. Hånell, T. Howells [et al.] // Journal of Intensive Care Medicine. – 2022. – Vol. 37, No. 11. – P. 1442-1450.

111. Bakaev, M. Intelligent information system to support decision-making based on unstructured web data / M. Bakaev, T. Avdeenko // ICIC Express Letters. – 2015. – Vol. 9, No. 4. – P. 1017-1023.

112. Blockchain-Enabled Joint Resource Allocation for Virtualized Video Service Functions / P. Yu, H. Zhao, K. Yang [et al.] // Security and Communication Networks. – 2022. – Vol. 2022. – P. 4349097.

113. Chen, Zh. Design of Computer Multimedia Intelligent Platform Using Big Data Analysis / Zh. Chen // Journal of Interconnection Networks. – 2022. – Vol. 22, No. Supp02.

114. Content-Based Medical Image Retrieval: A Survey of Applications to Multidimensional and Multimodality Data / A. Kumar, J. Kim, W. Cai [et al.] // Journal of Digital Imaging. – 2013. – Vol. 26, No. 6. – P. 1025-1039.

115. Costa, F. Multimodality and pronunciation in ICLHE (Integration of Content and Language in Higher Education) training / F. Costa, O. Mair // Innovation in Language Learning and Teaching. – 2022. – Vol. 16, No. 4-5. – P. 281-296.

116. Dosenko, A. Контент платформ: мультимодальний аспект / A. Dosenko // Держава та регіони. Серія: Соціальні комунікації. – 2023. – No. 2(54). – P. 94.

117. Duncan, J. Integrated Intelligence from Distributed Brain Activity / J. Duncan, M. Assem, S. Shashidhara // Trends in Cognitive Sciences. – 2020. – Vol. 24, No. 10. – P. 838-852.

118. Dynamic presence tracking system in shared environments / Sh. M. H. - , P. S. K. R. -, S. K. -, Dr. P. D. - // International Journal on Science and Technology. – 2025. – Vol. 16, No. 1.

119. Dzhurov, A. Advanced methods for detecting and blocking destructive content in text, images, and multimedia / A. Dzhurov, L. Cherkesova, E. Revyakina // Vesnik of Yanka Kupala State University of Grodno. Series 2. Mathematics. Physics. Informatics, Computer Technology and Control. – 2024. – Vol. 14, No. 3. – P. 131-143.

120. Hangloo, S. Combating multimodal fake news on social media: methods, datasets, and future perspective / S. Hangloo, B. Arora // Multimedia Systems. – 2022. – Vol. 28, No. 6. – P. 2391-2422.

121. Hordiichuk-Bublivska, O. Investigation of distributed matrix factorisation efficiency in the industrial systems / O. Hordiichuk-Bublivska // Information and communication technologies, electronic engineering. – 2023. – Vol. 3, No. 2. – P. 43-52.

122. Khan, M. I. Privacy Protection: YOLOv11 Face Detection and Blurring for GDPR Compliance in Hotels / M. I. Khan, V. B // Journal of Innovative Image Processing. – 2024. – Vol. 6, No. 4. – P. 397-417.

123. Kumar, M. V. Smart IoT based health care environment for an effective information sharing using Resource Constraint LLM Models / M. V. Kumar, G. P. Ramesh // Journal of Smart Internet of Things. – 2024. – Vol. 2024, No. 2. – P. 133-147.

124. Ladilova, A. Multimodal Metaphors of Interculturereality / Metaforas multimodais da interculturealidade / A. Ladilova // Revista de Estudos da Linguagem. – 2020. – Vol. 28, No. 2. – P. 917-955.

125. Li, Zh. Application and Challenge of Edge Computing Based on 5G Communication in Information and Communication Systems / Zh. Li, K. Cao // Journal of Electronic Research and Application. – 2024. – Vol. 8, No. 6. – P. 39-45.

126. Liu, Y. Distribution system outage information processing using comprehensive data and intelligent techniques / Y. Liu, 2002. – 1 p.

127. Netedu, L. Visual and verbal narration in the Romanian comic strips: rewriting canonic texts / L. Netedu // The Journal of Linguistic and Intercultural Education. – 2024. – Vol. 17, No. 2. – P. 67-83.

128. N. N. Teterin, N. Y. Borzykh, T. E. Smolentseva and A. V. Kalach, "Algorithm for Optimal Selection of a Strategy for Designing Corporate Information Systems Using Multi-criteria Optimization," 2024 4th International Conference on Technology Enhanced Learning in Higher Education (TELE), Lipetsk, Russian Federation, 2024, pp. 106-110.

129. Self-powered Biosensor Big Data Intelligent Information Processing System for Real-time Motion Monitoring / B. Liu, M. Shen, L. Mao [et al.] // Zeitschrift fur Anorganische und Allgemeine Chemie. – 2020. – Vol. 646, No. 11-12. – P. 500-506.

130. System-Information and Cognitive Technologies of Man-Made Infrastructure Cyber Security / L. S. Sikora, N. K. Lysa, Ye. I. Tsikalo, O. Yu. Fedevych // Journal of Cyber Security and Mobility. – 2023.

131. Wanselin, H. Analysing Multimodal Texts in Science—a Social Semiotic Perspective / H. Wanselin, K. Danielsson, S. Wikman // Research in Science Education. – 2022. – Vol. 52, No. 3. – P. 891-907.

ПРИЛОЖЕНИЕ А. СВИДЕТЕЛЬСТВА О ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММ ДЛЯ ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

RU 2025668422

(12) **ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ**

Номер регистрации (свидетельства):
2025668422

Дата регистрации: **15.07.2025**

Номер и дата поступления заявки:
2025667186 04.07.2025

Дата публикации и номер бюллетеня:
15.07.2025 Бюл. № 7

Контактные реквизиты:
teterin@mirea.ru

Автор:
Тетерин Николай Николаевич (RU)

Правообладатель:
Тетерин Николай Николаевич (RU)

Название программы для ЭВМ:
«Интеллектуальная информационная система обработки мультимодальных данных»

Реферат:
Программа позволяет выявлять деструктивное поведение за счет анализа различных типов данных. В программе предусмотрен анализ мультимодальных данных по типам: медиа и текст, только медиа или только текст. Представленная визуализация обработки мультимодальных данных позволяет сделать вывод о целесообразности применения интеллектуальной информационной системы на примере выявления деструктивного поведения пользователей.

Язык программирования: Python

Объем программы для ЭВМ: 13 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU 2025681455

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) **ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ**

Номер регистрации (свидетельства):
2025681455

Дата регистрации: **14.08.2025**

Номер и дата поступления заявки:
2025667282 04.07.2025

Дата публикации и номер бюллетеня:
14.08.2025 **Бюл. №** 8

Контактные реквизиты:
teterin@mirea.ru

Автор:
Тетерин Николай Николаевич (RU)

Правообладатель:
Тетерин Николай Николаевич (RU)

Название программы для ЭВМ:
«Интеллектуальная информационная система обработки данных в образовательной сфере»

Реферат:
Программа позволяет выявлять деструктивное поведение у студентов за счет анализа их групп в сети Интернет. В программе предусмотрен модуль рекомендации записи студента к психологу. Возможность программы визуализации обработки данных в образовательной сфере позволяет сделать вывод о целесообразности ее применения на примере выявления деструктивного поведения студентов. Тип ЭВМ: IBM PC-совмест. ПК; ОС: Windows.

Язык программирования: Python

Объем программы для ЭВМ: 47 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU 2025683295

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2025683295

Дата регистрации: **02.09.2025**

Номер и дата поступления заявки:
2025681803 20.08.2025

Дата публикации и номер бюллетеня:
02.09.2025 **Бюл. № 9**

Контактные реквизиты:
teterin@mirea.ru

Автор:
Тетерин Николай Николаевич (RU)

Правообладатель:
Тетерин Николай Николаевич (RU)

Название программы для ЭВМ:
«Программная реализация классификации цифровой обработки текстовых данных»

Реферат:
Программа позволяет классифицировать текст по заданным категориям для обеспечения безопасности. В программе представленный подход основан на выявлении деструктивного поведения пользователей в цифровой среде. Представленная визуализация классификации цифровой обработки текстовых данных позволяет сделать вывод о целесообразности инструментария для мониторинга и анализа деструктивных поведенческих паттернов среди пользователей на основе их цифровых коммуникаций. Тип ЭВМ: IBM PC-совмест. ПК; ОС: Windows.

Язык программирования: Python

Объем программы для ЭВМ: 29 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU 2025687164

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2025687164

Дата регистрации: **08.10.2025**

Номер и дата поступления заявки:
2025685512 24.09.2025

Дата публикации и номер бюллетеня:
08.10.2025 Бюл. № 10

Контактные реквизиты:
teterin@mirea.ru

Автор:
Тетерин Николай Николаевич (RU)

Правообладатель:
Тетерин Николай Николаевич (RU)

Название программы для ЭВМ:
«Программная реализация метода двухэтапной классификации контента»

Реферат:
Программная реализация метода двухэтапной классификации позволяет систематизировать процесс выявления угроз и повысить точность классификации контента. В программе представленный подход основан на двухэтапном анализе, где сначала выявляются характерные признаки контента, а затем рассчитывается условная вероятность. Представленная визуализация цифровой обработки данных позволяет сделать вывод о целесообразности, что предложенный метод представляет собой эффективный инструмент для интеллектуальных систем контент-модерации. Тип ЭВМ: IBM PC-совмест. ПК. ОС: Windows.

Язык программирования: Python

Объем программы для ЭВМ: 74 КБ

ПРИЛОЖЕНИЕ Б. АКТЫ О ВНЕДРЕНИИ

ООО «НПК «Карбон Групп»
309540, Россия, Белгородская обл.,
г. Старый Оскол, ст. Котел, Промузел,
пл. Прирельсовая, проезд М-4, стр. 7
Телефон: +7 (4725) 46-93-64
Факс: +7 (4725) 46-93-63
E-mail: carbon@carbon-group.ru
Сайт: www.carbon-group.ru

УТВЕРЖДАЮ:

Директор ООО «НПК «КарбонГрупп»

_____ Ж.М. Бендерская

«02» июня 2025 г.

АКТ

о внедрении результатов диссертационного исследования Тетерина Николая Николаевича «Разработка методов и средств интеллектуальной обработки мультимодальных данных из сети Интернет»

Комиссия в составе председателя – директор по развитию Петров Сергей Иванович; членов комиссии: ведущего специалиста Боевой Валентины Ивановны, юрисконсульта Корзуновой Марии Борисовны, настоящим актом подтверждает использование результатов диссертации Тетерина Николая Николаевича для анализа цифровых взаимодействий сотрудников ООО «НПК «КарбонГрупп».

Разработанный Тетериным Н.Н. метод обработки мультимодальных данных из сети Интернет для интеллектуальных систем используется в процессе анализа цифровых взаимодействий сотрудников на локальной платформе ООО «НПК «КарбонГрупп».

Председатель комиссии: Петров С.И.

Члены комиссии: Боева В.И.

Корзунова М.Б.

Общество с ограниченной ответственностью «АЙТИ КЛАСС»

ИНН 5003167092 КПП 500301001
Российская Федерация, 123007, г. Москва, Хорошёвское шоссе, 32А

Исх. № КЛ 010/25
На № от

УТВЕРЖДАЮ
Генеральный директор
_____И.С. Кожевников
«5» августа 2025

АКТ

о внедрении результатов диссертационного исследования Тетерина Николая Николаевича «Разработка методов и средств интеллектуальной обработки мультимодальных данных из сети Интернет»

Комиссия в составе председателя – директора по продукту Бексаева Николая Сергеевича; членов комиссии: аналитика данных Кончевского Артема Игоревича, системного аналитика Новосельцевой Екатерины Александровной, настоящим актом подтверждает использование результатов диссертации Тетерина Николая Николаевича для мониторинга корпоративных коммуникаций сотрудников ООО «АЙТИ КЛАСС».

Разработанный Тетериным Н. Н. кросс-модальный вероятностный метод классификации цифровой обработки аудио, текстовых данных, фото и видеоизображений контента используется в процессе мониторинга корпоративных коммуникаций в мессенджере ООО «АЙТИ КЛАСС».

Председатель комиссии: Бексаев Н. С.

Члены комиссии: Кончевский А. И.

Новосельцева Е. А.

УТВЕРЖДАЮ
Проректор по учебной работе
РТУ МИРЭА
доктор технических наук, профессор
_____ А.В. Тимошенко
«___» _____ 2025 г.

АКТ
о внедрении результатов диссертационного исследования
ТЕТЕРИНА НИКОЛАЯ НИКОЛАЕВИЧА
«Разработка методов и средств интеллектуальной обработки мультимодальных данных из сети Интернет», выполненного на соискание ученой степени кандидата технических наук по научной специальности 2.3.8. Информатика и информационные процессы, в образовательную деятельность Института информационных технологий федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА – Российский технологический университет»

Комиссия в составе председателя – директора Института информационных технологий, кандидата технических наук, доцента Зуева А.С.; членов комиссии: заведующего кафедрой инструментального и прикладного программного обеспечения, кандидата технических наук, доцента Болбакова Р.Г.; профессора кафедры прикладной математики, доктора технических наук, доцента Сараева П.В., настоящим актом подтверждает использование результатов диссертации Тетерина Н.Н. в образовательном процессе Института информационных технологий федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА – Российский технологический университет».

Полученные в рамках диссертации Тетерина Н.Н. результаты:

– метод обработки мультимодальных данных из сети Интернет для интеллектуальных систем;

– кросс-модальный вероятностный метод классификации цифровой обработки аудио, текстовых данных, фото и видеоизображений контента;

– архитектура интеллектуальной информационной системы обработки мультимодальных данных в цифровой среде;

используются при проведении практических занятий по дисциплинам «Проектирование аналитических систем», «Технологии и инструментарий анализа больших данных» профиля «Управление данными» направления подготовки 09.03.03 «Прикладная информатика» и профиля «Анализ данных» направления подготовки 01.03.04 «Прикладная математика».

Председатель комиссии:
директор Института информационных
технологий, кандидат технических наук, доцент А.С. Зуев

Члены комиссии:
заведующий кафедрой инструментального
и прикладного программного обеспечения,
кандидат технических наук,
доцент Р.Г. Болбаков

профессор кафедры прикладной
математики, доктор технических наук,
доцент П.В. Сараев