

## Анализ интернет-текстов с признаками информационных угроз при помощи больших языковых моделей

П. Д. Осокин<sup>1</sup>, С. А. Осокина<sup>2</sup>

*Алтайский государственный университет,*

*61 Lenin St., 656049, Barnaul, Russia. E-mail: <sup>1</sup>osokin@mail.asu.ru, <sup>2</sup>osokina@filo.asu.ru*

Статья направлена на верификацию гипотезы о способности современных больших языковых моделей ChatGPT и DeepSeek производить анализ текстов на естественном языке с целью выявления языковых средств, могущих свидетельствовать о наличии в них угрозы информационной безопасности, связанной с проявлениями экстремистской деятельности. Методологической основой исследования выступает принципиально новый подход к исследованию интернет-текстов посредством цифровых технологий с позиций информационной безопасности, с учетом юридических аспектов понимания сущности информационных угроз, в том числе угрозы экстремизма. Материалом анализа выступают 100 интернет-текстов на русском языке, представленные в открытом доступе в социальных сетях «ВКонтакте» и «Одноклассники», отобранные методом случайной выборки из открытых христианских сообществ в данных сетях. Семантический анализ отобранных текстов позволил распределить их в группы, отражающие проявление определенной субъективной тональности: нейтральные, одобряющие, оскорбляющие, осуждающие и содержащие резкую негативную оценку. Последние три группы попадают в зону риска наличия информационной угрозы. В результате анализа установлено, что обе системы – ChatGPT и DeepSeek – адекватно справляются с задачей выявления языковых средств, требующих дальнейшего анализа на предмет возможной угрозы информационной безопасности. Важно отметить, что данные, полученные в результате анализа, выполненного большими языковыми моделями, можно использовать только как дополнительный инструмент для формирования экспертной оценки текста на наличие признаков информационных угроз, которые помогают взглянуть на анализируемый текст более объективно, отдельно от личностных установок эксперта-человека. Однако окончательный вывод о наличии информационной угрозы вправе делать только эксперт-человек.

**Ключевые слова:** большая языковая модель, интернет-текст, тональность текста, информационная безопасность, информационная угроза.

## Analysis of Internet Texts with Signs of Information Threats Using Large Language Models

P. D. Osokin<sup>1</sup>, S. A. Osokina<sup>2</sup>

*Altai State University*

*Lenin St. 61, 656049, Barnaul, Russia. E-mail: <sup>1</sup>osokin@mail.asu.ru, <sup>2</sup>osokina@filo.asu.ru*

The article aims to verify the hypothesis about the ability of ChatGPT and DeepSeek language models to analyze natural language texts in order to identify language means that may indicate an information security threat associated with extremist activities. The methodological basis of the research is a fundamentally new approach to the study of Internet texts through digital technologies from the standpoint of information security, taking into account the legal aspects of information threats research, including the threat of extremism. The analyzed material consists of 100 Internet texts in the Russian language, publicly available on the social networks VKontakte and Odnoklassniki, selected by random sampling from these networks' open Christian communities. The semantic analysis of the selected texts allowed us to divide them into groups reflecting their subjective sentiment: neutral, approving, insulting, condemning and containing a strong negative assessment. The last three groups fall into the risk of containing an information threat. The research showed that both ChatGPT and DeepSeek systems adequately cope with the task of identifying language expressions that require further analysis for possible threats to information security. It is important to note that the responses given by Large Language Models can only be used as an additional instrument to support an expert assessment of the text for signs of information threats. This instrument helps to look at the analyzed text more objectively, separately from the personal attitudes of a human expert. However, only a human expert can make a final conclusion about the existence of an information threat.

**Key words:** Large Language Model, Internet text, sentiment analysis, information security, information threat.

## Введение

В эпоху стремительного развития цифровых технологий одним из актуальных направлений исследований становится изучение потенциала больших языковых моделей (Large Language Model, LLM) в различных направлениях языкознания, в том числе в сфере юрислингвистики.

Настоящее исследование направлено на изучение способности LLM анализировать интернет-тексты на наличие в них угроз информационной безопасности, в частности, признаков проявления экстремизма. Отнесение высказываний на определенном языке к экстремистским составляет одну из труднейших задач в области юрислингвистики [Королькова, Алексеева 2023; Куршакова, Рядчикова, Схалыхова 2023; Грушихина 2016], однако с ростом коммуникации посредством интернет-технологий данная проблема перемещается в сферу информационной безопасности и компьютерной лингвистики, поскольку анализу подвергаются публикации, размещенные в интернете.

В основе настоящего исследования лежит идея использования наиболее известных больших языковых моделей ChatGPT и DeepSeek для подтверждения или опровержения гипотезы о способности искусственного интеллекта (ИИ), существующего в виде сложных систем обработки больших массивов текстовых данных – больших языковых моделей, – производить анализ текстовых сообщений на предмет выявления характеристик, которые в дальнейшем могут получить правовую оценку как возможное проявление экстремизма.

Исследование приобретает дополнительную актуальность в свете внесения изменений и дополнений в «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 31.07.2025), связанных с установлением меры наказания за умышленный поиск материалов заведомо экстремистского содержания [КоАП РФ Статья 13.53 URL]. При этом под заведомо экстремистскими понимаются тексты, включенные в «Федеральный список экстремистских материалов», представленный на официальном сайте Министерства юстиции Российской Федерации<sup>1</sup>.

Данное лингвистическое исследование не предполагает обсуждение и толкование правовых норм, но поднимает вопрос о возможном наличии в случайно встречающихся интернет-сообщениях определенных языковых признаков, могущих иметь отношение к высказываниям экстремистского характера, которые способны формировать угрозы информационной безопасности.

Материалом для анализа послужили интернет-тексты, представляющие собой посты и комментарии к ним в популярных христианских сообществах в социальных сетях «ВКонтакте» и «Одноклассники» (проанализировано 100 случайно встретившихся текстов на русском языке).

## Методологические основания исследования

Проводимое исследование носит междисциплинарный характер. Поскольку работа направлена на выявление характеристик текстов, потенциально содержащих признаки информационных угроз экстремистского характера, исследование осуществляется на стыке юрислингвистики и информационной безопасности. Использование категориального аппарата информационной безопасности, в частности трактование наличия определенных языковых средств в тексте в качестве «угрозы», составляет научную новизну проводимого исследования. В частности, суть информационной безопасности как практической деятельности и научной дисциплины состоит в изучении способов предотвращения определенных информационных угроз и защиты от несанкционированных операций с информацией [Fullstack Academy 2025; Комов 2009; Юлдашев 2022], в том числе семантической информацией, передающейся языковыми знаками. При этом под угрозой в информационной безопасности понимается не факт совершения несанкционированного действия с информацией, существующей в том числе и в языковой форме, а наличие условий, которые потенциально могут привести к реализации такого действия [Joshi, Singh 2017: 129; TechTarget Contributor 2024]. Поскольку настоящее исследование направлено на изучение способности LLM определять наличие подобных условий в виде языкового материала в интернет-сообщениях, считаем использование категориального аппарата информационной безопасности в лингвистическом исследовании целесообразным и эффективным. В данном исследовании мы опираемся на наиболее полное понимание сущности информационной безопасности, представленное в «Доктрине информационной безопасности РФ», определяющее угрозу информационной безопасности как «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [Доктрина 2016: I, 26 URL]; в число таких действий входит информационное воздействие на сознание, связанное с экстремистской и террористической деятельностью [Доктрина 2016: III, 13 URL].

Определение сущности экстремизма представляет собой серьезную проблему в области российского и международного права. В первую очередь, при определении понятия экстремизма необходимо руководствоваться государственными нормативными актами определенной страны, в частности на территории Российской Федерации это Федеральный закон от 25 июля 2002 г. N114-ФЗ «О противодействии экстремистской деятельности». Однако, несмотря на то, что в законе перечислены определенные критерии, на деле весьма трудно доказать применительно к анализу языкового материала, можно ли рассматривать определенное высказывание как пропаганду, оправдание или одобрение противоправного действия. Деятельность лингвиста-эксперта в данном случае сводится к констатации наличия и характеристике определенных языковых средств в виде конкретных лексем, идиоматических выражений, грамматических конструкций, прагматики высказывания и тому подобного. Использование системы искусственного интеллекта в лингвистическом анализе может служить независимым объективным методом изучения языковых данных с целью установления факта наличия определенных языковых средств, в противовес и в дополнение к профессиональному анализу лингвистов-экспертов и юристов – конкретных личностей со своими ценностными установками.

Практическая значимость использования искусственного интеллекта в данном случае состоит в поиске внешних инструментов, свободных от личностных установок исследователя, для проведения анализа языкового материала,

<sup>1</sup> <https://minjust.gov.ru/ru/extremist-materials/>.

требующего получить определенную экспертную оценку. При совпадении результатов анализа, выполненного LLM, с результатами анализа человека-эксперта мы получаем дополнительное объективное свидетельство в виде оценки текста искусственным интеллектом. Однако, подчеркнем, результаты, представленные ИИ, могут носить характер только дополнительного (вспомогательного) инструмента анализа. Окончательное суждение о наличии/отсутствии в высказывании определенных языковых средств, соотносимых с видами информационных угроз, может вынести только человек.

### Результаты и обсуждение

Наиболее трудной задачей является установление спектра языковых средств, свидетельствующих о формировании угрозы информационной безопасности в виде языкового проявления экстремизма. Полагаем, что для решения данной проблемы перспективным является использование методов исследований, направленных на определение тональности текста (sentiment analysis, opinion mining) [Bing 2010]. Анализ тональности текста предполагает выявление языковых маркеров определенной субъективной тональности, проявляющейся в виде конкретных лексем или выражений с оценочной семантикой. Необходим контент-анализ большого массива текстов, комплексный семантический анализ в сочетании с анализом контекста и прагматической направленности высказывания.

В частности, лексико-семантический анализ предполагает выявление текстов, в которых содержатся определенные лексемы, имеющие отношение к семантическому полю «экстремизм» и смежным полям: «раса», «национальность», «язык», «религия», «оправдание», «одобрение», «пропаганда» и подобных – примерный перечень таких семантических полей можно составить путем лингвистического анализа текста вышеупомянутого федерального закона.

Для воссоздания спектра слов, ассоциирующихся с данными семантическими полями, представляется эффективным использование ресурса «Карта слов» (Kartaslov.ru), на котором содержится множество объединений слов и словосочетаний, связанных с заданным словом. Например, по запросу «оправдание» ресурс выдает более 100 ассоциативно связанных слов, синонимов и выражений, среди которых: *правда, суд, ложь, оправдываться, вина, извинение, адвокат, человек, приговор, неправда, подсудимый* и другие. Контекстуальный анализ предполагает выявление «соседства» слов из указанных семантических полей (с одной стороны – «раса», «национальность», «язык», «религия», с другой – «оправдание», «одобрение», «суд», «ложь», «вина») в узком и широком контекстах. Прагматический анализ необходим для установления намерений автора, которые могут передаваться наличием эмоционально окрашенных слов, особых синтаксических конструкций, при помощи иных средств.

На предварительном этапе анализа был произведен отбор интернет-текстов, содержащих лексемы из перечисленных выше семантических полей, и исследована общая тональность данных текстов. Сначала производилось ранжирование отобранных текстов экспертом-человеком, а затем полученные результаты сопоставлялись с результатами анализа, выполненного LLM. Полученные результаты во многом совпали с результатами других исследований, направленных на изучение тональности текста машинными средствами, и подтвердили общую эффективность использования систем искусственного интеллекта для анализа текста (в частности, подобные выводы делаются в работе [Овсянникова 2025]).

Семантический анализ отобранных нами текстов позволил распределить их в группы, отражающие проявление определенной субъективной тональности:

- 1) нейтральные тексты (примерно 8% от общего числа проанализированных текстов);
- 2) тексты с одобрительной оценкой (примерно 50%);
- 3) осуждающие тексты, как правило, содержащие аргументацию (примерно 20%);
- 4) тексты с явно выраженной негативной оценкой (примерно 12%);
- 5) оскорбляющие тексты (примерно 10%).

Приведенное процентное соотношение текстов относительно, поскольку выделенные группы представляют собой пересекающиеся множества. Один и тот же текст может входить в несколько групп одновременно.

Нейтральные тексты, как правило, представляют собой короткие посты информационного характера, не содержащие в явном виде языковых средств, требующих дальнейшего анализа на предмет обнаружения угроз информационной безопасности. В текстах с одобрительной оценкой не обнаружено высказываний, которые можно было бы проинтерпретировать как одобряющие противоправные действия.

Тексты оскорбляющие, осуждающие и содержащие негативную оценку, по нашему мнению, попадают в зону риска наличия информационных угроз в виде нагнетания конфликтных ситуаций, в том числе с потенциальными признаками экстремистского содержания. Данные тексты далее были загружены для анализа в системы DeepSeek и ChatGPT. При этом обеим системам задавался вопрос «Носит ли данный текст экстремистский характер». В результате анализа обе системы отнесли 8 текстов к потенциально экстремистским, требующим дальнейшего изучения с точки зрения широкого контекста их создания и прагматических установок авторов. Остальные тексты были определены как содержащие негативное мнение или нейтральное мнение, выражающее религиозную позицию, что относительно коррелирует с группами, выделенными нами на этапе отбора и предварительного лингвистического анализа.

Приведем конкретные примеры текстов с разной языковой тональностью.

Ниже представлен Текст 1, который на этапе предварительного лингвистического анализа был отнесен нами к типу текстов осуждающего характера и, одновременно, содержащих резкую негативную оценку, однако не содержащих прямых призывов к противоправным действиям в виде глаголов в повелительном наклонении и иных языковых средств:

*«Шарлотаны, обманываете других людей ничего невинно не подозревающих, грешите как хотите и тем самым обманываете себя что вы с Богом, Бог он не такой ,Он другой ,Он свет и Он абсолютно свят ,а вы грешите ,странно какому вы богу поклоняетесь? праведен суд на вас от Бога»* (здесь и далее интернет-тексты скопированы в авторском написании).

На рисунках 1 и 2 представлены результаты анализа данного текста системами DeepSeek и ChatGPT.



Данное высказывание содержит резкую критику в адрес определенной группы людей, обвиняя их в обмане и грехе, а также утверждает, что над ними будет "праведный суд от Бога". Однако оно **не содержит прямых призывов к насилию, ненависти или дискриминации по этническим, религиозным или социальным признакам.**

#### Оценка на экстремизм:

**✗ Не является экстремистским** в юридическом понимании (например, по ст. 282 УК РФ), так как:

- Нет **прямых угроз** или призывов к враждебным действиям.
- Критика носит **религиозно-морализаторский** характер, а не направлена на разжигание ненависти к группе людей.
- Используются **богословские формулировки** ("праведен суд от Бога"), а не агрессивная риторика.

#### ⚠ Но важно учитывать контекст:

Если подобные высказывания используются для систематического **унижения верующих** или подстрекательства к конфликту, они могут привлекать внимание правоохранительных органов.

**Вывод:** Само по себе это высказывание **не экстремистское**, но его тональность может считаться резкой или оскорбительной в зависимости от ситуации.



Рис. 1. Результат анализа Текста 1 при помощи DeepSeek

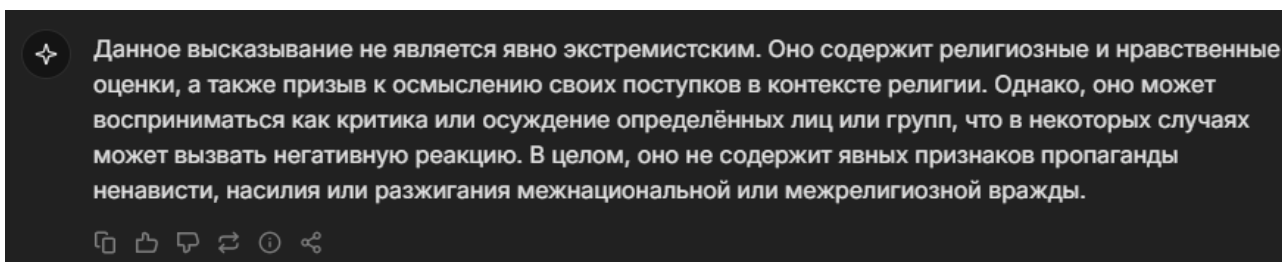


Рис. 2. Результат анализа Текста 1 при помощи ChatGPT

Стоит отметить, во-первых, аргументированность оценки, предоставленной DeepSeek: ссылку на действующее законодательство страны, на государственном языке которой задан промпт-вопрос, и пункты, по которым проводилась оценка; во-вторых, сноску о необходимости принятия во внимание контекста, в котором применяется данный текст. Также внимания заслуживает вывод LLM, крайне близко совпадающий с результатами предварительного анализа для данного интернет-текста. ChatGPT показал меньшую полноту анализа, аргументации и отсутствие ссылок на источники, что ставит данную оценку ниже, чем предоставленную DeepSeek.

Анализ Текста 2, содержащего фразу «<...> чтоб этим тварям церковным руки отрубили чтоб не поднимали руки на пожилых людей» позволяет выявить более яркие языковые признаки нагнетания конфликтной ситуации. В частности, текст содержит употребление слова *тварь* в адрес служителей церкви в значении «подлый человек», которое сопровождается в словарях русского языка пометой «презрительное» [Грамота.ру 2000–2025 URL]. Такое употребление слова придает тексту ярко выраженную оскорбляющую семантику и негативную оценку. Употребление глаголов в форме прошедшего времени, которая в данном случае приобретает семантику сослагательного наклонения со значением желаемого действия, в определенной степени можно проинтерпретировать как призыв к осуществлению действия.

На рисунках 3 и 4 представлены результаты анализа данного текста системами ChatGPT и DeepSeek. Анализ DeepSeek, как и в предыдущем примере, выделяется большей полнотой и точностью аргументации.



Да, данное высказывание **можно расценить как экстремистское** по следующим причинам:

1. **Призыв к насилию** – фраза "чтоб этим тварям церковным руки отрубили" содержит явное желание причинения физического вреда определенной группе людей (церковным служителям).
2. **Дезориентация и агрессия** – слова "тварям церковным" выражают крайнюю степень ненависти и унижения в адрес религиозных деятелей.
3. **Обобщение и подстрекательство** – утверждение строится на негативном стереотипе о всех представителях церкви, что может разжигать вражду.

## Вывод

Текст нарушает нормы против экстремизма, так как содержит **призыв к насилию и унижительную риторику** в отношении религиозной группы. В ряде стран подобные высказывания могут быть основанием для правовых последствий.

Если вам нужен более нейтральный способ выразить критику, можно переформулировать мысль без оскорблений и угроз.



Рис. 3. Результат анализа текста «В отличие от церкви...» при помощи DeepSeek

✦ Данное высказывание содержит выражение негативного отношения и оскорбительные слова в адрес представителей церкви, а также призыв к насилию ("чтоб этим тварям церковным руки отрубили"). Такие выражения могут быть признаны экстремистскими, поскольку они пропагандируют насилие и разжигают ненависть по религиозному признаку. Поэтому, скорее всего, это высказывание можно считать экстремистским.

Рис. 4. Результат анализа текста «В отличие от церкви...» при помощи ChatGPT

Однако необходимо обратить внимание на то, что выражение *отрубить руки*, которое обе LLM охарактеризовали как призыв к осуществлению насильственного физического действия, может употребляться в русском языке не только в своем прямом значении, но и в качестве образного идиоматического выражения для усиления эмоциональной составляющей речи, а не призыва к конкретному физическому действию. Поэтому далее необходим более тщательный анализ прагматической составляющей высказывания экспертом-человеком.

Таким образом, проделанный анализ позволяет заключить, что системы ChatGPT и DeepSeek на современном этапе их разработки в целом адекватно интерпретируют языковые данные, поскольку результаты их анализа во многом совпадают с анализом, выполненным профессиональным лингвистом, но формируемые системами ответы можно использовать только в качестве вспомогательного инструмента для дальнейшего лингвистического анализа. Отметим, что для проведения исследования использовались базовые версии систем ChatGPT и DeepSeek, что позволяет сделать вывод о возможности более эффективного применения данных систем в случае использования их расширенных версий.

Принципиально важно подчеркнуть, что обнаружение в проанализированных текстах определенных языковых средств в виде негативно маркированных слов, стилистически сниженной или оценочной лексики, побудительных грамматических конструкций не является достаточным основанием для заключения о наличии/отсутствии в высказывании признаков экстремизма. Однако наличие указанных языковых средств свидетельствует о возможности формирования угрозы информационной безопасности в данном сообществе пользователей социальной сети. Формирование угрозы происходит при систематическом появлении подобных текстов и их бесконтрольном распространении в виде репостов.

## Заключение

Большие языковые модели демонстрируют высокий потенциал для анализа текстов в качестве дополнительного вспомогательного инструмента в работе лингвиста-эксперта на предмет выявления информационных угроз экстремистского характера. Для повышения точности анализа требуется:

- дополнительное обучение моделей на специализированных датасетах;
- интеграция контекстного анализа (учет культурных и языковых нюансов);
- привлечение экспертов для финальной оценки спорных случаев.

Данное исследование вносит вклад в развитие инструментов автоматизированного мониторинга интернет-контента, что актуально для обеспечения информационной безопасности. Проведенное исследование может быть адаптировано для анализа других типов информационных угроз (мошенничество, дезинформация, кибербуллинг), а его результаты могут быть использованы для модерации социальных сетей или проведения комплексных исследований угроз, проявляющихся в виде языковой информации. В перспективе исследования входит также изучение этических и правовых оснований для



использования больших языковых моделей в рамках анализа информационных угроз и общей тональности интернет-текстов.

## Литература

- Грамота.ру, 2000–2025. URL: [https://gramota.ru/poisk?query=тварь&mode=slovari&dicts\[\]=42](https://gramota.ru/poisk?query=тварь&mode=slovari&dicts[]=42)
- Грушихина В. А. Судебная психолого-лингвистическая экспертиза текста (на примере дела об экстремизме) / Деятельность правоохранительных органов в современных условиях. Сборник материалов XXI международной научно-практической конференции. – Иркутск, 2016. – С. 12–15.
- Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. URL: [https://www.mid.ru/ru/foreign\\_policy/official\\_documents/1539546/](https://www.mid.ru/ru/foreign_policy/official_documents/1539546/).
- КоАП РФ Статья 13.53. Поиск заведомо экстремистских материалов и получение доступа к ним, в том числе с использованием программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_34661/d698a1c3214cb529c29991c00154e985d9d7f607/](https://www.consultant.ru/document/cons_doc_LAW_34661/d698a1c3214cb529c29991c00154e985d9d7f607/)
- Комов С. А. Термины и определения в области информационной безопасности. Москва, 2009.
- Королькова А. В., Алексеева М. И. Лингвистическая экспертиза текстов, публично оправдывающих терроризм и/или экстремизм / Филологические науки. Вопросы теории и практики. – 2023. – Т. 16. – № 8. – С. 2339–2343.
- Куршакова Т. Д., Рядчикова Е. Н., Схалыхова С. Ш. Языковые маркеры экстремизма, фашизма, нацизма: из практики судебных лингвистических экспертиз / Казанская наука. – 2023. – № 6. – С. 27–33.
- Овсянникова М. А. Анализ тональности текста посредством инструмента искусственного интеллекта / Три «Л» в парадигме современного гуманитарного знания: Лингвистика, Литературоведение, Лингводидактика. Москва, 2025. С. 33–38.
- Юлдашев Ж. Б. К определению сущности международной информационной безопасности / Коммуникология: электронный научный журнал. – 2022. – Т. 7. – № 4. – С. 115–125.
- Bing Liu. Sentiment Analysis and Subjectivity / Handbook of Natural Language Processing (англ.) / под ред. N. Indurkha и F. J. Damerau. 2010. URL: <https://www.cs.uic.edu/~liub/FBS/NLP-handbook-sentiment-analysis.pdf>
- Fullstack Academy, LLC. What is Information Security? 2025. URL: <https://www.fullstackacademy.com/blog/what-is-information-security>
- Joshi Ch., Singh U.K. Information security risks management framework – A step towards mitigating security risks in university network / Journal of Information Security and Applications. – 2017. – No. 35. – Pp. 128–137. doi:10.1016/j.jisa.2017.06.006.
- TechTarget Contributor, 2024, Top 10 types of information security threats for IT teams, URL: <https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams>.

## References

- Article 13.53 of the Administrative Code of the Russian Federation. Searching for knowingly extremist materials and gaining access to them, including using hardware and software to access information resources, information and telecommunication networks, access to which is restricted. Available from: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_34661/d698a1c3214cb529c29991c00154e985d9d7f607](https://www.consultant.ru/document/cons_doc_LAW_34661/d698a1c3214cb529c29991c00154e985d9d7f607) (in Russian).
- Bing Liu. (2010). Sentiment Analysis and Subjectivity. Handbook of Natural Language Processing <https://www.cs.uic.edu/~liub/FBS/NLP-handbook-sentiment-analysis.pdf>
- Fullstack Academy, LLC (2025). What is Information Security? Available from: <https://www.fullstackacademy.com/blog/what-is-information-security>.
- Gramota.ru, 2000–2025. URL: [https://gramota.ru/poisk?query=тварь&mode=slovari&dicts\[\]=42](https://gramota.ru/poisk?query=тварь&mode=slovari&dicts[]=42) (in Russian).
- Grushihina, V.A. (2016). Forensic psychological and linguistic examination of the text (using the case of extremism as an example). The activity of law enforcement agencies in modern conditions. Collection of materials of the XXI International scientific and practical conference, 12–15 (in Russian).
- Joshi, Ch., Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. Journal of Information Security and Applications, 35, 128–137. doi:10.1016/j.jisa.2017.06.006.
- Komov, S. A. (2019). Terms and definitions in the field of information security. Moscow (in Russian).
- Korolkova, A. V., Alekseeva, M. I. (2023). Linguistic examination of the texts publicly justifying terrorism and/or extremism. Philology. Theory & Practice, 16, 8, 2339–2343 (in Russian).
- Kurshakova, T. D., Ryadchikova, E. N., Skhalyakhova, S. Sh. (2023). Linguistic markers of extremism, fascism, Nazism: from the practice of forensic linguistic examinations. Kazan Science, 6, 27–33 (in Russian).
- Ovsyannikova, M. A. (2025). Text tonality analysis using an artificial intelligence tool. Three "L" in the paradigm of modern humanitarian knowledge: Linguistics, Literary Studies, Linguodidactics. Moscow, 33–38 (in Russian).
- TechTarget Contributor, 2024, Top 10 types of information security threats for IT teams, Available from: <https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams>.
- The Information Security Doctrine of the Russian Federation. Approved by Decree of the President of the Russian Federation No. 646 dated December 5, 2016. Available from: [https://www.mid.ru/ru/foreign\\_policy/official\\_documents/1539546/](https://www.mid.ru/ru/foreign_policy/official_documents/1539546/). (in Russian).
- Yuldashev, Zh. B. (2022). Towards the definition of the essence of international information security. Kommunikologiya: electronic scientific journal, 7, 4, 115–125 (in Russian).

**Citation:**

Осокин П. Д., Осокина С. А. Анализ интернет-текстов с признаками информационных угроз при помощи больших языковых моделей // Юрислингвистика. – 2025 – 38. – С. 74-80.

Osokin P. D., Osokina S. A. (2025) Analysis of Internet Texts with Signs of Information Threats Using Large Language Models. Legal Linguistics, 38, 74-80.



This work is licensed under a Creative Commons Attribution 4.0. License