DOI: https://doi.org/10.25146/1995-0861-2022-61-3-354

УДК 159.9

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В СОЦИАЛЬНЫХ МЕДИА

Н.А. Богульская (Красноярск, Россия)
М.М. Кучеров (Красноярск, Россия)
В.Б. Туговиков (Красноярск, Россия)
А.С. Сабило (Красноярск, Россия)

Аннотация

Проблема и цель. В современном мире информация и информационно-коммуникационные технологии играют большую роль во всех сферах жизни общества и государства. При этом Интернет не только дает новые возможности, но и может оказывать деструктивное воздействие на пользователей, в основном на молодежь. *Цель* исследования – выявление возможностей обеспечения информационно-психологической безопасности в интернет-пространстве.

Методология исследования основана на подходах к автоматической фильтрации контента социальных медиа.

Результаты исследования. Анализируются и сравниваются подходы к автоматизации обнаружения запрещенного контента в Интернете. Обосновывается выбор метода для проведения вычислительного эксперимента и сделаны выводы по результатам его проведения.

Заключение. В статье приведены результаты исследований по проблеме автоматизированной процедуры обнаружения и фильтрации в интернет-пространстве запрещенного законодательством РФ контента.

Ключевые слова: *Интернет, молодежь, информационно-психологическая безопасность, автоматическая фильтрация, алгоритмы классификации.*

Богульская Нина Александровна – кандидат физико-математических наук, доцент института космических и информационных технологий, Сибирский федеральный университет (Красноярск); e-mail: nbogulskaya@sfu-kras.ru
Кучеров Михаил Михайлович – кандидат физико-математических наук, доцент института космических и информационных технологий, Сибирский федеральный университет (Красноярск); e-mail: mkucherov@sfu-kras.ru
Туговиков Виктор Борисович – кандидат физико-математических наук, доцент института космических и информационных технологий, Сибирский федеральный университет (Красноярск); e-mail: vtugovikov@sfu-kras.ru
Сабило Ангелина Сергеевна – студентка института космических и информационных технологий, Сибирский федеральный университет (Красноярск); e-mail: sabilo2000@mail.ru

Постановка проблемы. Информационно-психологическая безопасность личности – это состояние защищенности человека от негативных информационных воздействий и внедрения деструктивной информации в сознание или подсознание индивида, позволяющих специальными средствами и методами воздействовать на психику и, как следствие, определять его поведение [Хириев, 2007].

Информационно-психологическое воздействие на личность как инструмент достижения определенных целей существует столько, сколько существует человечество. Подобные воздействия предпринимаются не только для рекламы товаров, создания брендов и т.д., но и для утверждения авторитета в коллективах, сообществах отдельными его членами. Это касается и учебных заведений. Однако большая часть обучающейся

молодежи не обладает личностной зрелостью в юношеском возрасте и требует к себе, помимо организационных моментов учебного процесса, дополнительного внимания по развитию личностных качественных характеристик: способностей, самосознания, сознания, жизненной позиции [Селезнева, Белая, Грузинцев, 2021].

Если еще в начале XXI в. монополия на воздействие на массовое сознание людей принадлежала средствам массовой информации и деятелям культуры, то в настоящее время человечество переживает этап бурного и неконтролируемого роста числа объектов информационно-психологического воздействия на сознание людей. Основной целью такого воздействия в подавляющем большинстве случаев является максимальное извлечение прибыли за счет монетизации популярности, раскрутки товаров и услуг и т.п. К этому стремятся как отдельные блогеры, так и крупные медийные корпорации. Известно, что наиболее эффективным способом привлечения внимания к тому или иному событию или объекту является агрессивный контент, который призван пробуждать в человеке чувство страха, агрессии, неприятия, иные негативные эмоции, выводящие личность из состояния спокойствия и душевного равновесия. При этом создателей такого информационного продукта не интересуют педагогические и воспитательные аспекты информационно-психологического воздействия подобного контента на детей и подростков. IT-инфраструктуру для достижения политических и военных целей используют и специальные подразделения разведок всех стран мира, центры специальных психологических операций при силовых ведомствах.

На защиту граждан Российской Федерации, а в первую очередь подрастающего поколения, призвано встать законодательство. Так, на уровне Конституции Российской Федерации уже заложены нормы, которые определяют правовые основы защиты от негативного информационного воздействия, принципы законности, баланс интересов личности, общества, государства и, конечно же, бизнеса. В контексте данной статьи следует отметить, что положения Конституции РФ направлены на противодействие распространению следующих видов информации:

– контент, рассчитанный на разжигание ненависти, вражды и насилия;

– заведомо ложная реклама, прочая противоречащая традиционным устоям ложная информация;

– информация, посягающая на честь и достоинство граждан;

– информация, которая оказывает негативное воздействие на здоровье и духовно-нравственное состояние людей.

Следующим по значимости документом является Доктрина информационной безопасности, утвержденная указом Президента РФ № 464 от 05.12.2016. Данный документ среди основных целей определяет необходимость нейтрализации информационно-психологических воздействий, направленных против таких важных исторических основ, как патриотизм, любовь к родине, защита Отечества (ст. 21 д). Доктрина в качестве участников процесса обеспечения защиты от вредоносного информационно-психологического воздействия определяет: средства массовой информации, операторов связи, владельцев телекоммуникаций, социальных сетей, разработчиков программного обеспечения, связанных с развлекательным и информационным контентом, и т.д.

Одним из основных уровней обеспечения конституционных прав и свобод граждан Российской Федерации является развитие законодательной базы, направленной на обеспечение информационно-психологической безопасности личности [Конституция РФ]. Так, российские законодатели утвердили ряд поправок в Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации». В частности, статья 10.6 закона № 149-ФЗ посвящена конкретизации порядка принятия мер по ограничению доступа к информации, размещенной с нарушением требований российского законодательства [РФ. Законы № 149-ФЗ, 2006]. В целях повышения ответственности за распространение вредоносного контента и информации, оказывающей негативное воз-

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

действие на личность человека, особенно молодых людей, вводятся новые меры ответственности в Гражданский и Уголовный кодекс РФ [РФ. Законы № 195-ФЗ, № 63-ФЗ, 2022; № 530-ФЗ, 2020].

Обзор научной литературы. Проблема автоматического распознавания текстов имеет глубокую историю [Леонтьева, 2006]. Обеспечение информационно-психологической безопасности личности возможно в двух аспектах. К первому из них относится ограничение доступа к деструктивной информации, ко второму – формирование внутренней защиты личности от восприятия разрушительной информации или ее нейтрализации и обесценивания [Пантелеев, 2014]. Типичным примером первого из подходов служит блокировка доступа к нежелательным сайтам, при которой происходит сопоставление IP-адресов с их доменными именами и закрывается доступ к сайту. В этих целях возможно применение указанных выше законодательных мер.

Блокирование контента, который может представлять угрозу информационно-психологической защищенности личности, имеет запаздывающий характер. Сайт с деструктивным содержанием должен просуществовать некоторое время и быть посещаемым, после чего он будет признан как опасный в информационном плане. Проблема состоит в том, чтобы разработать такое программное обеспечение, которое позволило бы обнаруживать угрозы в реальном масштабе времени.

Проблемой методологии автоматического анализа текстов служат неопределенность смыслового восприятия текста, невозможность найти однозначное соответствие между содержанием исходного текста и результатом его понимания субъектом. По мнению Н.Н. Леонтьевой, обрабатываемый в процессе автоматического понимания текста массив должен быть снабжен гипертекстовой системой, причем в уже имеющихся программах обработки гипертекстовые связи проставляются, как правило, человеком [Леонтьева, 2006].

В работе [Maasberg et al., 2020] обращается внимание на патологические черты личности как один из трех основных факторов, предрасполагающих людей к злонамеренному опасному поведению наряду с подходящей возможностью (ситуацией) и состоянием внутреннего кризиса. Они составляют так называемую «темную триаду»: макиавеллизм, нарциссизм и психопатия. По мнению одного из источников [Дробницкий, 1974], на всем протяжении развития морального сознания внутренним стержнем и структурой его изменения является возникающий конфликт между возвышенным идеалом и практическим расчетом, нравственным долгом и непосредственным желанием, который существует всегда и проявляется во всех сторонах жизни. Таким образом, циничное поведение авторов и распространителей сетевой агрессии объясняется дефектом морального сознания, проявления которого представляют угрозу информационно-психологической защищенности личности.

На практике применяется в основном статистический контент-анализ по отдельным лексическим единицам, гипотетически связанным с информационной опасностью текста. Как отмечалось [Ермаков, 2002], трудности достижения необходимого качества прикладных систем объясняются дефицитом включения лингвистической составляющей в алгоритмы, доминированием статистических методов.

Из вышесказанного можно сделать вывод, что сочетание контент-анализа, контекст-анализа и классификации эмоциональной тональности позволяет создать предпосылку для алгоритмизации процедуры компьютерного анализа текста.

Методология исследования основана на подходах к автоматической фильтрации контента социальных медиа. Использованы теоретические методы исследования: анализ, синтез, систематизация научных идей.

Результаты исследования. В статье выполнены анализ и сравнение подходов, позволяющих автоматизировать процесс фильтрации запрещенного контента социальных медиа. Обосновывается выбор метода для проведения вычислительного эксперимента и сделаны выводы по результатам его проведения.

Согласно закону № 149-ФЗ размещение на страницах сайтов нецензурной лексики должно

ограничиваться [РФ. Законы № 149-ФЗ, 2006]. Алгоритм работы блокировки текста при этом достаточно прост: цикл сравнивает фразу со словами из словаря нецензурной лексики, который заранее был составлен из различных словарей русской нецензурной лексики [Ковалев, 2005; Мокиенко, Никитина, 2007].

Но часто нецензурная лексика отсутствует, при этом текст содержит явную или скрытую агрессию, оскорбления. В этом случае можно создать классификатор тональности текста.

Все эмоции можно разделить на два больших класса: негативные и позитивные. Если классификатор покажет, что текст относится к позитивному классу эмоций, то его можно публиковать или пропускать при мониторинге контента. Если же классификатор укажет негативную тональность, необходимо вручную проверить текст на наличие агрессии или оскорблений одного пользователя в сторону другого и при необходимости заблокировать данный пост, комментарий или сообщение [Худякова, Давыдов, Васильев, 2012].

Несмотря на достаточно большое число алгоритмов и методов классификации эмоций в тексте, все они основываются всего на двух подходах к созданию модели представления текста и двух подходах к непосредственному распознаванию эмоций [Котельников, Окулов, 2012; Turney, 2002].

Подход на основе словарей, в котором для представления текста используются специальные словари, в основном это словари эмоциональной лексики, а также словари синонимов, антонимов, акронимов. При этом в модели представления текста остаются только те слова исходного текста, которые присутствуют в словарях эмоциональной лексики, возможно, расширенных словами из словарей синонимов, антонимов и акронимов [Ковалев, 2005].

Подход на основе корпусов, при котором модель представления текста создается на основе статистического анализа текстового корпуса (коллекции), содержащего тексты, заранее размеченные в соответствии с решаемой задачей. При этом каждому слову может быть присвоена эмоциональная оценка, обозначающая, например, его тональность, определяемую на основе отношения количества положительных и отрицательных текстов, в которые входит данное слово.

При распознавании (классификации) эмоций применяются два основных подхода: лексический и на основе машинного обучения. Оба подхода используют модель представления текста, построенную либо при помощи словарей, либо на основе корпусов.

Лексический подход предполагает, что эмоции, выраженные в тексте, можно определить путем подсчета эмоциональных оценок слов, входящих в данный текст. Окончательное решение осуществляется при помощи некоторой функции, например разности между суммами эмоциональных оценок слов положительной и отрицательной тональностей.

На основе некоторых данных в процессе машинного обучения осуществляется автоматическое построение классифицирующей функции. Машинное обучение является традиционным подходом в задаче текстовой классификации [Pang, Lee, Vaithyanathan, 2002; Tang et al., 2010]. Данные, на которых происходит обучение, могут представлять собой размеченную коллекцию текстов (обучение с учителем) или, например, словарь слов с эмоциональными оценками, который используется для автоматической разметки текстов (обучение без учителя).

Известны несколько эффективных алгоритмов классификации тональности текста, например наивный байесовский классификатор [Шагин, 2022; Наивный..., 2022], метод опорных векторов, сверточные нейронные сети [Lai et al., 2015]. Для вычислительного эксперимента был выбран наивный байесовский классификатор [Tan et al., 2009]. Программа была написана на языке Python. Наивный байесовский классификатор делает вывод об агрессивности или позитивности анализируемого текста с помощью вероятностной функции, где высчитывает вероятность тональности отдельного слова, основываясь на его вхождениях в позитивные или негативные фразы обучающей коллекции.

Первым этапом алгоритма является лематизация исходного текста – приведение слов к их лемме. Лемма – это нормальная (словар-

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

ная) форма слова. Для глаголов и деепричастий леммой является инфинитив, для прилагательных – единственное число, именительный падеж, мужской род, для существительных – единственное число, именительный падеж.

Следующей и достаточно трудоемкой задачей стало составление обучающей коллекции, на основе которой классификатор учится и делает выводы о тональности анализируемого текста. Эта коллекция содержит фразы, которые часто можно встретить в виде комментариев и постов пользователей социальных сетей, фразы из обыденной жизни и непосредственную оценку позитивности или агрессивности каждой фразы.

Исходя из результатов работы, можно сделать вывод, что метод машинного обучения с учителем во многом зависит от качества размеченной обучающей коллекции. Поэтому главной задачей данной работы было создание четкой, грамотной и отнесенной к нужной тематике словаря и обучающей текстовой коллекции.

Заключение. Статья содержит обоснование актуальности проблемы мониторинга контента социальных медиа. Приведены ссылки, которые подтверждают, что законодательство РФ обязывает блокировать запрещенный контент. В работе сделаны обзор и сравнение подходов к автоматизации процесса анализа эмоциональной окраски текста. Обосновывается выбор метода классификации для проведения вычислительного эксперимента. Для вычислительного эксперимента был выбран наивный байесовский классификатор. Программа была написана на языке Python. Вычислительный эксперимент показал зависимость качества классификации от объема и качества обучающей коллекции.

Как показывает практика, многие социальные сети и сайты не имеют систем фильтрации агрессивного текстового контента, несмотря на то, что такой контент должен быть заблокирован по законодательству РФ. Поэтому продолжение исследований в данном направлении актуально и будет иметь практическое применение владельцами социальных сетей и цифровых образовательных сред. А знакомство с информационными технологиями детей и подростков должно начинаться с усвоения правил поведения в интернет-пространстве.

Библиографический список

1. Доктрина информационной безопасности (утверждена указом Президента РФ № 464 от 05.12.2016).
2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
3. Российская Федерация. Законы: Федеральный закон от 27.07.2006 № 149-ФЗ: редакция от 30 декабря 2021 г.: с изменениями и дополнениями,вступившими в силу с 1 января 2022 г. // КонсультантПлюс: справочная правовая система. URL: http://www.consultant.ru/document/cons docLAW 61798/a3cba9a7 c2ac9aa487df2d4172734dd5139376f5/ (дата обращения: 20.06.2022).
4. Российская Федерация. Законы. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30.12.2001 № 195-ФЗ: редакция от 11 июня 2022 г. // КонсультантПлюс: справочная правовая система. URL: http://www.consultant.ru/document/cons doc LAW 34661/ d40cbd099d17057d9697b15ee8368e49953416ae/ (дата обращения: 20.06.2022).
5. Российская Федерация. Законы. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ: редакция от 25 марта 2022 года // КонсультантПлюс: справочная правовая система. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/d350878ee36f956a74c2c86830d066eafce20149/ (дата обращения: 20.06.2022).
6. Российская Федерация. Законы. Федеральный закон от 30.12.2020 № 530-ФЗ // КонсультантПлюс: справочная правовая система. URL: http://www.consultant.ru/document/cons doc LAW 372700/ (дата обращения: 20.06.2022).
7. Дробницкий О.Г. Понятие морали. М.: Наука, 1974. 386 с.

8. Ермаков А.Е. Компьютерная лингвистика и анализ текста // Мир ПК. 2002. № 9. URL: http://www.osp.ru/peworld/2002/ 09/163968 (дата обращения: 20.05.2022).
9. Ковалев Г.Ф. Русский мат – следствие уничтожения табу // Культурные табу и их влияние на результат коммуникации: сб. науч. тр. Воронеж: ВГУ, 2005, С. 184–197.
10. Котельников Е.В., Окулов С.М. Обзор подходов для автоматического распознавания эмоций в текстах // Научные итоги года. 2012. № 2. С. 96–101. URL: https://cyberleninka.ru/article/n/obzor-podhodov-dlya-avtomaticheskogo-raspoznavaniya-emotsiy-v-tekstah/viewer (дата обращения: 20.05.2022).
11. Леонтьева Н.Н. Автоматическое понимание текстов: системы, модели, ресурсы. М.: Академия, 2006. 304 с.
12. Мокиенко В.М., Никитина Т.Г. Русское сквернословие. Краткий, но выразительный словарь. М.: Олма Медиа Групп, 2007. 384 с.
13. Наивный байесовский классификатор. URL: https://ru.wikipedia.org/wiki/Наивныйбайесовскийклассификатор (дата обращения: 20.06.2022).
14. Пантелеев А.Ф. Анализ текста как средство обеспечения информационной безопасности личности // Информационная безопасность регионов: научно-практический журнал. 2014. № 1 (14). С. 32–38.
15. Селезнева Н.Т., Белая А.А., Грузинцев А.В. Психологические факторы использования личностью сетевых коммуникаций // Вестник КГПУ им. В.П. Астафьева. 2021. № 4 (58). С. 44–53. URL: https://elibrary.ru/download/elibrary47411591578574 91.pdf
16. Хириев А.Т. Теоретико-методологические основы информационной безопасности личности. 2007 (на правах рукописи). URL: https://www.daaudit.ru/news-pubs/pub-2-1.html
17. Худякова М.В., Давыдов С., Васильев В.Г. Классификация отзывов пользователей с использованием фрагментных правил. Компьютерная лингвистика и интеллектуальные технологии: по матер. ежегодной Междунар. конфр. «Диалог». Бекасово, 30 мая – 3 июня 2012 г. М.: Изд-во РГГУ, 2012. Вып. 11 (18): в 2 т. Т. 2: Доклады специальных секций.
18. Шагин А. Наивный байесовский классификатор. URL: https://medium.com/nuances-of-programming/наивный-байесовский-алгоритм-все-что-нужно-о-нем-знать-85f6e04c3b74 (дата обращения: 20.06.2022).
19. Lai S., Xu L., Liu K., Zhao J. Recurrent convolutional neural networks for text classification. In: Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence. January 25–31, 2015. Austin, Texas USA, 2015. Is. 29 (1). P. 2267–2273.
20. Maasberg M., Van Slyke C., Ellis S., Beebe N. The dark triad and insider threats in cyber security // Communications of the ACM. 2020. Vol. 63, No. 12. P. 64–80. URL: https://cacm.acm.org/magazines/2020/12 (access date: 20.05.2022).
21. Pang B., Lee L., Vaithyanathan S. Sentiment classification using machine learning techniques. In: Proceedings of the ACL-02 Conference on «Empirical methods in natural language processing». Association for Computational Linguistics, 2002. Vol. 10. P. 79–86.
22. Tan S., Cheng X., Wang Y., Xu H. Adapting naive Bayes to domain adaptation for sentiment analysis. In: Boughanem, M., Berrut, C., Mothe, J., Soule-Dupuy, C. (eds) Advances in Information Retrieval. ECIR 2009. Lecture Notes in Computer Science. Vol. 5478. P. 337–349. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-00958-7_31
23. Tang X. Yang C., Wong Y., Wei C. Understanding online consumer review opinions with sentiment analysis using machine learning // Pacific Asia Journal of the Association for Information Systems. 2010. No. 3 (2). P. 73–89.
24. Turney P.D. Thumbs up or thumbs down? Semantic orientation applied to unsupervised classification of reviews. In: Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics, Philadelphia, Pennsylvania, 2002. P. 417–424.

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА

DOI: https://doi.org/10.25146/1995-0861-2022-61-3-354

APPROACHES TO ENSURING INFORMATION SECURITY AND PSYCHOLOGICAL SAFETY IN SOCIAL MEDIA

N.A. Bogulskaya (Krasnoyarsk, Russia)
M.M. Kucherov (Krasnoyarsk, Russia)
V.B. Tugovikov (Krasnoyarsk, Russia)
A.S. Sabilo (Krasnoyarsk, Russia)

Abstract

Statement of the problem. In the modern world, information and information technologies play an important role in all spheres of society and the state. At the same time, the Internet not only provides new opportunities, but can also have a destructive effect on users, mainly young people.

The purpose of the study is to identify the possibilities of ensuring information security and psychological safety in the Internet space.

The research methodology is based on approaches to automatic filtering of social media content.

Research results. Approaches to detecting prohibited content on the Internet are analyzed and compared. The choice of a method for conducting a computational experiment is substantiated and conclusions are drawn based on the results of its implementation.

Conclusion. The article presents results of the research on the problem of an automated procedure for detecting and filtering content prohibited by the legislation of the Russian Federation on the Internet.

Keywords: *Internet, youth, information security, psychological safety, automatic filtering, classification algorithms.*

Bogulskaya Nina A. – PhD (Physics and Mathematics), Associate Professor, Institute of Space and Information Technologies, Siberian Federal University (Krasnoyarsk, Russia); e-mail: nbogulskaya@sfu-kras.ru
Kucherov Mikhail M. – PhD (Physics and Mathematics), Associate Professor, Institute of Space and Information Technologies, Siberian Federal University (Krasnoyarsk, Russia); e-mail: mkucherov@sfu-kras.ru
Tugovikov Viktor B. – PhD (Physics and Mathematics), Associate Professor, Institute of Space and Information Technologies, Siberian Federal University (Krasnoyarsk, Russia); e-mail: vtugovikov@sfu-kras.ru
Sabilo Angelina S. – BA Student, Institute of Space and Information Technologies, Siberian Federal University (Krasnoyarsk, Russia); e-mail: sabilo2000@mail.ru

References

1. Information Security Doctrine approved by the Decree of the RF President No. 464 dated 05.12.2016.
2. The Constitution of the Russian Federation (adopted by a nationwide vote on 12/12/1993 with amendments approved during the All-Russian vote on 07/01/2020).
3. Russian Federation. Laws: Federal Law No. 149-FZ dated July 27, 2006: edition of December 30, 2021: with amendments and additions that came into force on January 1, 2022. In: Consultant Plus: legal reference system. URL: http://www. consultant.ru/document/consdocLAW61798/a3cba9a7c2ac9aa487df2d4172734 dd51 39376f5/
4. Russian Federation. Laws. Code of the Russian Federation on Administrative Offenses: Federal Law No. 195-FZ of December 30, 2001: edition of June 11, 2022. In: Consultant Plus: reference legal system. URL: http://www.consultant.ru/ document/cons doc LAW 34661/ d40cbd099d17057 d9697b15ee8368e49953416ae
5. Russian Federation. Laws. Criminal Code of the Russian Federation: Federal Law of June 13, 1996 No. 63-FZ: edition of March 25, 2022. In: Consultant Plus: reference legal system. URL: http://www.consultant.ru/document/consdocLAW10699/ d350878ee36f956a74c2c86830d066eafce20149/
6. Russian Federation. Laws. Federal Law of December 30, 2020No. 530-FZ. In: Consultant Plus: reference legal system. URL: http://www.consultant.ru/ document/cons doc LAW 372700/

7. Drobnitsky O.G., The concept of morality. Moscow: Nauka, 1974. 386 p.
8. Ermakov A.E. Computer Linguistics and Text Analysis // Mir PK (World of Personal Computers). 2002. No. 9. URL: http://www.osp.ru/ peworld/2002/09/163968
9. Kovalev G.F. Russian obscene words – a consequence of the abolition of taboos. In: Cultural taboos and their influence on the result of communication: Collection of scientific papers. Voronezh: VGU, 2005. P. 184–197.
10. KotelnikovE.V., Okulov S.M. Review of approaches for automatic recognition of emotions in texts // Nauchnye itogi goda: dostizheniya, proekty, gipotezy (Scientific Annual Results: Achievements, Projects, Hypotheses. 2012. No. 2. P. 96–101. URL: https://cyberleninka.ru/article/n/obzor-podhodov-dlya-avtomaticheskogo-raspoznavaniya-emotsiy-v-tekstah/viewer
11. Leontyeva N.N. Automatic understanding of texts: systems, models, resources. Moscow: Akademia, 2006. 304 p.
12. Mokienko V.M., Nikitina T.G. Russian profanity. A short but expressive dictionary. Moscow: Olma Media Grupp, 2007. 384 p.
13. Naive Bayes classifier. In: Wikipedia. URL: https://en.wikipedia.org/wiki/Naïve Bayes classifier
14. Panteleyev A.F. Text analysis as a way of ensuring privacy // Informatsionnaya bezopasnost regionov (Information Security of Regions). 2014. No. 1 (14). P. 32–38.
15. Selezneva N.T., Belaya A.A., Gruzintsev A.V. Psychological factors in the use of network communications by a person // Vestnik KGPU im. V.P. Astafyeva (Bulletin of the KSPU named after V.P. Astafyev). 2021. No. 4 (58). P. 44–53. URL: https://elibrary.ru/download/elibrary 47411591 57857491.pdf
16. Khiriev A.T. Theoretical and methodological foundations of privacy (PhD Thesis Manuscript). 2007. URL: https://www.daaudit.ru/news-pubs/pub-2-1.html
17. Vasilyev V.G., Khudyakova M.V., Davydov S. Sentiment classification by fragment rules. In: Proceedings of the International Conference “Dialogue”. Bekasovo, 30 May – 3 June 2012. Moscow: Izdatelstvo RGGU, 2012. Is. 11 (18), vol. 2. P. 66.
18. Shagin A. Naïve Bayes classifier. URL: https://medium.com/nuances-of-programming/наивный-байесовский-алгоритм-все-что-нужно-о-нем-знать-85f6e04c3b74 (access date: 20.06.2022).
19. Lai S., Xu L., Liu K., Zhao J. Recurrent convolutional neural networks for text classification. In: Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence. January 25–31, 2015. Austin, Texas USA, 2015. Is. 29 (1). P. 2267–2273.
20. Maasberg M., Van Slyke C., Ellis S., Beebe N. The dark triad and insider threats in cyber security // Communications of the ACM. 2020. Vol. 63, No. 12. P. 64–80. URL: https://cacm.acm.org/magazines/2020/12 (access date: 20.05.2022).
21. Pang B., Lee L., Vaithyanathan S. Sentiment classification using machine learning techniques. In: Proceedings of the ACL-02 Conference on “Empirical methods in natural language processing”. Association for Computational Linguistics, 2002. Vol. 10. P. 79–86.
22. Tan S., Cheng X., Wang Y., Xu H. Adapting naive Bayes to domain adaptation for sentiment analysis. In: Boughanem, M., Berrut, C., Mothe, J., Soule-Dupuy, C. (eds) Advances in Information Retrieval. ECIR 2009. Lecture Notes in Computer Science. Vol. 5478. P. 337–349. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-00958-7_31
23. Tang X. Yang C., Wong Y., Wei C. Understanding online consumer review opinions with sentiment analysis using machine learning // Pacific Asia Journal of the Association for Information Systems. 2010. No. 3 (2). P. 73–89.
24. Turney P.D. Thumbs up or thumbs down? Semantic orientation applied to unsupervised classification of reviews. In: Proceedings of the 40th Annual Meeting of the Association for Computational Linguistics, Philadelphia, Pennsylvania, 2002. P. 417–424.

ВЕСТНИК КРАСНОЯРСКОГО ГОСУДАРСТВЕННОГО ПЕДАГОГИЧЕСКОГО УНИВЕРСИТЕТА им. В.П. АСТАФЬЕВА