Юрислингвистика

Legal Linguistics, 2025, 36, 74-81, doi: https://doi.org/10.14258/leglin(2025)3613

ЛИНГВОЭКСПЕРТОЛОГИЯ *УДК 81'33, ББК 81.1, ГРНТИ 16.31.61, Код ВАК 5.9.8*

Цифровые социальные угрозы: от лингвистики до криминалистики в зеркале патентных решений

И. Д. Мамаев[1, 2], М. А. Марусенко[3], В. В. Петров[4]

[1]Балтийский государственный технический университет «Военмех» им. Д. Ф. Устинова
ул. 1-я Красноармейская, 1, 190005, Санкт-Петербург, Россия. E-mail: mamaev_id@voenmeh.ru
Санкт-Петербургский государственный университет
Университетская наб., д. 11, 199034, Санкт-Петербург, Россия. E-mail: [2]i.mamaev@spbu.ru, [3]m.marusenko@spbu.ru
[4]22-я линия Васильевского Острова, 7, 199105, Санкт-Петербург, Россия. E-mail: vadim.petrov@spbu.ru

В условиях роста цифровых угроз и трансформации криминальных практик критически важной задачей для обеспечения безопасности становится выявление социально опасных сообществ. Данная статья представляет собой систематизированный обзор 15 российских и международных патентов периода 2014–2023 гг., которые посвящены технологиям определения деструктивных групп и поведений в цифровом пространстве. Детально проанализированы патентные решения, сгруппированные по пяти ключевым направлениям: лингвистический анализ текстов, криминалистическая экспертиза данных, моделирование профилей пользователей, биометрическая идентификация и контроль нежелательной активности. Установлено, что 47% патентов защищают алгоритмические методы. Выявлены ключевые технологические тренды: доминирование лингвистических методов (анализ ключевых выражений и семантических паттернов) и прогнозирование угроз с помощью моделирования поведения пользователей. При этом сохраняются серьезные ограничения: фрагментарность модулей, недооценка междисциплинарности и этических рисков, которые связаны с обработкой персональных данных. Особое внимание уделено патентам, в которых описаны подходы по анализу психофизиологических реакций или краудсорсинговой модерации конфликтов. Подчеркивается необходимость синтеза криминалистики и систем компьютерной лингвистики для создания адаптивных систем определения деструктивных сообществ. Результаты исследования имеют практическую ценность для разработчиков, правоохранительных органов и патентных экспертов.

Ключевые слова: криминалистика, социально опасные сообщества, преступные сообщества, преступность в Интернете, корпусная лингвистика, патентоспособность.

Digital Social Threats: From Linguistics to Forensic Science in the Mirror of Patent Solutions

I. D. Mamaev[1, 2], M. A. Marusenko[3], V. V. Petrov[4]

[1]Baltic State Technical University "Voenmeh" named after D.F. Ustinov
1 1st Krasnoarmeyskaya, 190005, St. Petersburg, Russia. E-mail: mamaev_id@voenmeh.ru
St. Petersburg State University
11 Universitetskaya Emb., 199034, St. Petersburg, Russia. E-mail: [2]i.mamaev@spbu.ru, [3]m.marusenko@spbu.ru
[4]7 22nd Line V.O., 199105, St. Petersburg, Russia. E-mail: vadim.petrov@spbu.ru

Since digital threats and the transformation of criminal practices are going forward at a steady pace, the detection of socially dangerous communities is becoming a crucial task for ensuring security. The paper presents a systematic review of 15 Russian and international patents (2014–2023) concerning technologies for detecting destructive groups and behaviors in the digital space. Patents are analyzed in detail, they are grouped into five key areas: linguistic analysis of texts, forensic data examination, user profile modeling, biometric identification, and control of unwanted activity. It has been established that 47% of patents protect algorithmic methods. The key technological trends that are identified are as follows: the dominance of

linguistic methods (analysis of key expressions and semantic patterns) and threat prediction using user behavior modeling. At the same time, serious limitations are described: fragmentation of modules, underestimation of interdisciplinarity and ethical risks associated with the processing of personal data. Particular attention is paid to patents that describe approaches to analyzing psychophysiological reactions or crowdsourcing conflict moderation. The need for synthesizing forensics and computer linguistics systems to create adaptive detection systems is emphasized. The results of the study are of practical value for developers, law enforcement agencies, and patent experts.

Key words: forensic science, socially dangerous communities, criminal communities, Internet crime, corpus linguistics, patentability.

Выявление социально опасных групп является ключевой задачей обеспечения безопасности современного общества и предотвращения криминальных угроз. Развитие информационно-коммуникационных технологий и увеличение объемов информации, которые проходят через цифровые платформы, создают серьезные вызовы для обнаружения и нейтрализации потенциальных угроз [Артамонов, Артамонова, Сафонов 2022]. *«Современное развитие информационных технологий неизбежно повлекло трансформацию всех сфер жизни человека, общества и государства. Также это коснулось и преступности, которая всегда оперативно адаптирует в свои криминальные схемы любые современные технологии, включая информационные, что породило новые виды общественно опасных посягательств…»* [Пристансков, Харатишвили, Евстратова 2023: 587]. Одна из наиболее перспективных областей, которая позволяет решить данную задачу, – разработка запатентованных инновационных методов и устройств.

Патенты в аспекте рассматриваемой задачи, с одной стороны, представляют собой инструмент защиты интеллектуальной собственности разработчиков [Кочеткова 2022], с другой – являются источником информации для анализа тенденций и определения уровня технологического прогресса в данной области [Вьет, Кравец 2022]. Патентный анализ позволяет определить перспективные ниши для внедрения инновационных решений. Выявление социально опасных групп в глобальной сети Интернет требует комплексного подхода, который объединяет достижения в области технологий обработки больших данных, компьютерной лингвистики и криминалистики. Многие из таких решений уже модульно находят отражение в патентах, которые защищают способы мониторинга социальных сетей (см., например, [RU 2701990 C1]) или способы анализа поведения пользователей (см., например, [WO/2018/124931]). Особое внимание уделяется разработке систем, способных автоматизировать процесс предсказания возможной опасности (см., например, [RU 2658165 C2]), что потенциально может поспособствовать формированию профильной базы данных для профилактики потенциально опасных пользователей правоохранительными органами.

Цель настоящей статьи – систематизация и изучение содержания патентов, зарегистрированных на территории Российской Федерации, которые описывают способы и устройства определения социально опасных групп. Основной акцент направлен на выявление ключевых направлений исследований, описание технологий и методов, а также анализ их применимости в реальной практике. В работе рассмотрены как патенты, которые предлагают инновационные подходы к решению данной задачи, так и те, которые демонстрируют существующие недостатки и ограничения используемых методов. Актуальность темы обусловлена увеличением числа угроз, связанных с деятельностью социальных групп в глобальной сети Интернет, которые способны дестабилизировать общественное спокойствие (ряд статистических показателей за последние пару лет приведены на аналитических медиаплатформах «Ростелеком-Солар» [Ростелеком-Солар URL], Positive Technologies [Positive Technologies URL] и др.), и необходимостью разработки эффективных решений для их обнаружения. Анализ патентов в этом направлении предоставляет ценную информацию не только для научного сообщества, но и для разработчиков, стремящихся улучшить существующие методы.

Предлагаемая методология параметризации патентов, восходящая к идеям параметризации текстовых массивов [Захаров, Азарова 2012; Косова 2020], основана на анализе описаний пятнадцати патентов, которые связаны с разработкой технологий, направленных на обработку опасной текстовой информации, анализ пользовательского поведения, выявление мошеннической активности и обеспечение безопасности данных. Патенты отобраны из баз данных «Роспатент» [Роспатент URL] и PATENTSCOPE [PATENTSCOPE URL] посредством поиска по таким ключевым словам и выражениям, как «онлайновые сообщества», «информационная безопасность», «идентификация сообществ» и др. Тексты одновременно охватывают области криминалистики и лингвистики, что и определило направление методологии.

В процессе работы проведена декомпозиция функционала способов и технологий на более мелкие элементы, которые затем группировались в укрупненные направления (Таблица 1).

Таблица 1 – Декомпозиция патентов

Основные направления	**Параметры**
Лингвистический анализ	Идентификация лексико-семантических признаков текстов, анализ коммуникативных актов, идентификация спам-текстов и фишинг-текстов, анализ голосовых сообщений
Криминалистический анализ	Определение отклонений от предписываемого поведения, совершение преступлений с использованием социальной инженерии, нарушение информационной безопасности, соблюдение родительского контроля, оценка

Основные направления	**Параметры**
	угроз безопасности.
Моделирование поведения и профилей пользователей	Описание структуры социальных связей и пользовательских поведений, выявление онлайн-сообществ, социальная параметризация цифровых личностей на основе личных данных.
Биометрический анализ	Биометрическая идентификация, психофизиологическая и общая диагностика состояния здоровья.
Контроль нежелательной активности	Обнаружение нежелательных звонков, контроль коммуникаций.

Разработанный подход позволил описать исследуемые патенты в терминах параметров в Таблице 2.

Таблица 2 – Матрица «Патент-Параметры»

Патент	**Лингвистический анализ**	**Криминалистический анализ**	**Моделирование поведения и профилей**	**Биометрический анализ**	**Контроль нежелательной активности**
RU2658165		+			
RU2559725			+		
RU2469389			+		
RU177377		+			
RU2256223				+	
WO/2020/176003					+
WO/2014/163524	+		+		
RU2701990	+	+			
RU2580027	+	+			
RU2790946		+			
WO/2018/124931	+		+		+
RU2790330	+	+			
RU2634180	+				
RU2719553	+				
RU2780046	+	+			+

Большинство патентов защищают способы (методы, алгоритмы), что характерно для IT-сферы, так как гибкость описания позволяет авторам адаптировать предложенные методы под различные платформы. В данном случае под платформой понимается «совокупность технологий и спецификаций, обеспечивающая аппаратную и/или программную совместимость различных продуктов» [Викисловарь URL]. Треть патентов представлена смешанным типом, что характерно для задач одновременной фиксации и алгоритма, и процесса его интеграции в инфраструктуру. Общая статистика по патентам приведена на рисунке 1.

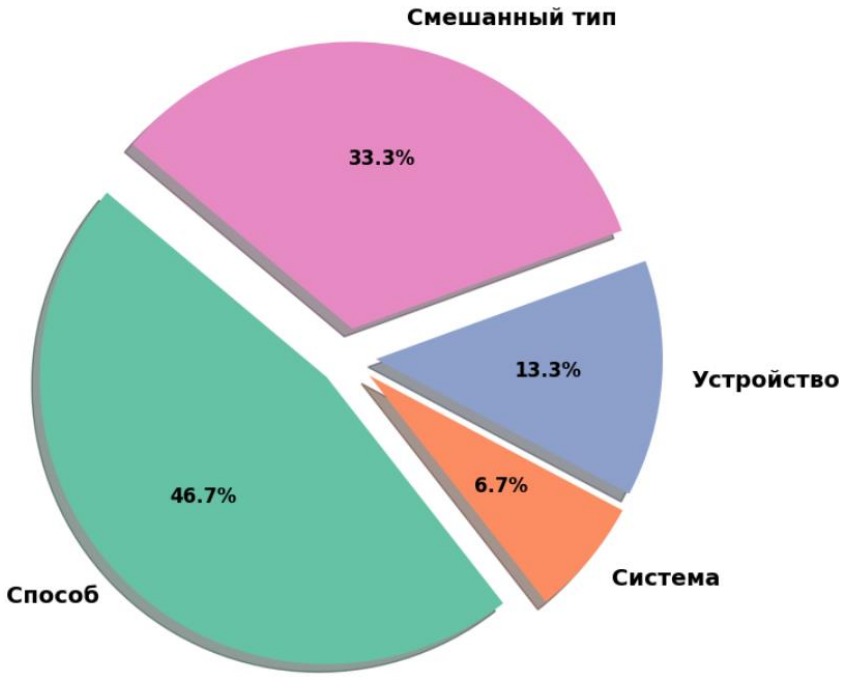

Рисунок 1 – Распределение патентов по типам изобретений

Далее приведем сравнительные характеристики патентов по каждому из представленных направлений.

Патенты по направлению лингвистического анализа

В патенте RU2580027 «Система и способ формирования правил поиска данных, используемых для фишинга» основное внимание сосредоточено на выявлении фишинговых угроз путем обработки различных типов данных: текстов, гиперссылок и мультимедиа. Система сначала классифицирует полученные данные, а затем проводит их лингвистический анализ для поиска ключевых признаков фишинга. Важная часть системы – выявление слов и фраз из предопределенного списка, которым присваиваются весовые коэффициенты, что позволяет оценивать степень угрозы. Лексический анализ проводится и в патенте WO/2014/163524 «Способ составления виртуального портрета пользователя», в котором посредством выделения определенных слов и словосочетаний определяется возможность предоставления пользователю услуги или кредита. В патенте RU2701990 «Способ использования системы определения тематики документов для целей информационной безопасности» акцентируется внимание на предварительной лемматизации текстов, которая упрощает последующий лексический анализ. После этого система сравнивает приведенные к базовой форме лексемы с классифицированной базой терминов и определяет тематику документа. Если содержание документа совпадает с запрещенными категориями, доступ к такому контенту блокируется. Патент RU2580027 примечателен интеграцией лингвистического анализа с мультимедийно-сетевой обработкой, что помогает выявлять даже сложные фишинговые атаки и оперативно формировать правила их обнаружения. RU2701990, напротив, отличается точной тематической классификацией текстов и устойчивостью к языковым вариациям благодаря использованию методов лемматизации.

К указанной лингвистической группе также относятся патенты WO/2018/124931 «Способ минимизации конфликтов во взаимоотношениях между людьми в средствах коммуникации», RU2790330 «Способ определения фишингового электронного сообщения», RU2634180 «Система и способ определения сообщения, содержащего спам, по теме сообщения, отправленного по электронной почте», RU2719553 «Способ содержательного анализа текстовой информации» и RU2780046 «Компьютерное устройство для определения нежелательного звонка». Так, в RU2790330C2 и RU2634180 применяются элементы семантических анализаторов – классификаторы (алгоритм логистической регрессии, метод опорных векторов и пр.) и векторные модели дистрибутивной семантики соответственно. WO/2018/124931 также предполагает процедуру анализа текста, но в явном виде она не прописана, однако основной акцент смещается в сторону визуальной модальности. RU2719553 среди рассматриваемых патентов выделяется внедрением процедур, близких к задачам профилирования автора письменного текста: на основании процентов служебных слов, содержащихся в текстах, коэффициентов лексического разнообразия, коэффициентов логической связности, средних длин слов и средних длин предложений проводятся расчеты и делается вывод о наличии или отсутствии единого автора для рассматриваемых текстов. При этом все раскрытые ранее патенты имеют дело с письменной формой текста, а устройство, описанное в патенте RU2780046, имеет дело как со звуковым сигналом, так и с последующим его преобразованием в письменную продукцию для применения упомянутых в данном разделе языковых эвристик.

Патенты по направлению криминалистического анализа

Рассмотренные патенты связаны с решением разных криминалистических подзадач с помощью алгоритмов автоматизированного анализа данных. Патенты RU2658165 «Способ и устройство для уведомления об аномальной видеоинформации» и RU2790946 «Способ и система анализа голосовых вызовов на предмет выявления и предотвращения социальной инженерии» работают с аудиовизуальным материалом. Первым способом определяются аномалии в видео: например, опасные предметы или изображения замаскированных личностей, а при

применении второго способа распознаются мошеннические схемы посредством анализа аудиопотока. Оба способа полезны для оперативного реагирования на признаки преступления, но их эффективность зависит от качества поступающих данных. В частности, изображение низкого качества или фоновый/технический шум в аудиосигнале могут спровоцировать ложное срабатывание систем и/или устройств.

RU177377 «Устройство определения интересов ребенка и оценки уровня угроз ребенку в интернете» и RU2701990 связаны с фильтрацией контента. В RU177377 оценивается уровень угроз для детей в сети Интернет, отслеживаются посещенные ресурсы, а в RU2701990 описывается процедура блокировки доступа к мошенническим веб-страницам. К сожалению, внедрение новых форм подачи запрещенного контента, в том числе и сгенерированных при помощи систем искусственного интеллекта, остается незамеченным.

Группа патентов RU2580027, RU2790330 и RU2780046 направлена на борьбу с фишинговыми киберпреступлениями. Их общая черта – многоэтапная проверка входных данных.

Патенты по направлению моделирования поведения и профилей

Патент RU2559725 «Система моделирования виртуального сообщества пользователей» ориентирован на инженерную оптимизацию виртуальных сообществ посредством обработки транзакций в режиме реального времени, сама система в явном виде не затрагивает поведенческие компоненты. В отличие от него, в патенте RU2469389 «Способ интеграции профилей пользователей онлайновых социальных сетей» решается проблема интеграции профилей из разнородных социальных сетей с помощью модели Условных Случайных Полей (Conditional Random Field, CRF) и метрики строковой/графовой близости. Этот подход автоматизирует сопоставление данных, что особенно актуально в эпоху неоднозначности цифровых личностей, которые интерпретируются как искусственно созданные виртуальные подобия живых людей [Будылина 2024] с возможной фальсификацией их аккаунтов на просторах сети Интернет. Патент WO/2014/163524 также рассматривает виртуальное портретирование пользователя, но для задачи оценки кредитоспособности. Предложенным способом анализируются социальные связи и кредитная история, что позволяет прогнозировать поведение пользователя. В свою очередь, в патенте WO/2018/124931 посредством системы цветовых блок-знаков вводится возможность моделирования конфликтного состояния онлайн-сообщества.

К достоинствам рассматриваемых патентов с позиции социомоделирования можно отнести, в частности, способ модерации сообществ, затрагиваемый в WO/2018/124931. Данный способ основан на коллективном участии, что повышает вовлеченность пользователей. Тем не менее возникают и вопросы этического характера. В патенте WO/2014/163524 при анализе кредитной истории игнорируются вопросы конфиденциальности, что противоречит Федеральному закону от 27.07.2006 «О персональных данных» № 152-ФЗ [Федеральный закон от 27.07.2006 «О персональных данных» № 152-ФЗ URL]. Таким образом, в патентах отражена эволюция моделирования поведения и профилей пользователей, начиная от решения задач технической оптимизации (RU2559725) и переходя к социально-ориентированным решениям (WO/2018/124931). С нашей точки зрения, перспективным способом моделирования мог бы стать тот, который сочетает как алгоритмическую точность (RU2469389), так и возможности краудсорсинга (WO/2018/124931). Вместе с тем для этого требуется решить вопросы защиты приватности и минимизировать субъективные искажения.

Патенты по направлению биометрического анализа

Конечно, выявление социально опасных групп проводится и по биометрическому «портрету» человека. Среди рассматриваемых патентов только один из представленных в корпусе имеет данную направленность – RU2256223 «Способ комплексной идентификации личности человека, паспортного контроля и диагностики текущего психофизиологического состояния личности и компьютерная система для его осуществления». Авторы описывают применение реакций на визуальные, аудиальные и тактильные стимулы и физиологических показатели (например, пульс) для контроля текущего состояния пользователя. Данный патент хоть и ориентирован, по мнению создателей, на автоматизированную проверку людей на пропускных пунктах, однако сфера его распространения, по нашему мнению, более широкая. В частности, анализ одинаковых или близких психофизиологических пользовательских «портретов» позволит выявить группы с радикальными взглядами, враждебным восприятием окружающего мира или преступным поведением.

Патенты по направлению контроля нежелательной активности

В RU2780046 предлагается система для анализа голосовых вызовов с целью идентификации спам-звонков. Предложенная технология основана на многоуровневом подходе, при котором на первом этапе анализируются параметры вызова, такие как идентификационный номер абонента и пространственно-временные характеристики, а затем, при необходимости, проводится детальное описание потоковых данных. Этот подход позволяет минимизировать как ложные срабатывания, так и пропуски нежелательных звонков. В патенте WO/2018/124931 расширяется область применения: охватываются электронные письма и другие виды цифровых данных. Техническая реализация ориентирована на использование клиентских приложений и сервисов, которые анализируют сообщения непосредственно на устройствах пользователей или на уровне почтовых серверов. Наконец, в патенте WO/2020/176003 «Способ контроля конфиденциальности коммуникаций с пользователями» понятие активности пользователя рассматривается с позиции «цифрового следа», которое, как верно отмечает Д. А. Свиридов, рассматривается как вид «информации, которая сохраняется после совершения действий в мобильных сетях, глобальной сети Интернет, локальных сетях, а также отдельных технических устройствах» [Свиридов 2023]. Пользователь может включить режим скрытой коммуникации с другим пользователем. Все действия пользователя («следы» в виде реакций на онлайн-публикацию, ее перепост и пр.) в рамках этой коммуникации не видны другим

пользователям. Похожий подход реализуется в приложениях, организующих доступ в Dark Net, в которых, согласно К. П. Маляновой, «невозможна систематическая слежка за пользователями» [Малянова 2023: 91].

Таким образом, основная проблема существующих патентов – сохранение дистанции между теоретическими возможностями алгоритмов и практическими потребностями правоохранительных органов, которые сталкиваются с необходимостью расследования киберпреступлений. Для уменьшения этой дистанции в разрабатываемых патентах необходимо объединение методов традиционного языкознания, криминалистики и машинного обучения, что позволит создать инструменты, которые смогут не только обнаруживать угрозы, но и одновременно прогнозировать эскалацию конфликтов и осуществлять их профилактику. Существующим патентам также не хватает междисциплинарной интеграции и устойчивости к новым вызовам, среди которых – социально опасные сообщества, которые используют технологии генеративного искусственного интеллекта. «Следы» сгенерированных текстовых продукций, будь то расшифровка телефонного звонка или копия электронного сообщения, в перспективе можно определить посредством проецирования методов стилеметрии и лингвистического профилирования на существующие методы выявления опасных сообществ.

Тем не менее, открытым вопросом, на наш взгляд, остается взаимодействие между разрабатываемыми корпусами для выявления сообществ и этичностью. Технологии, агрегирующие персональные данные, должны учитывать существующие правовые нормы. Разработка этических стандартов для оценки повысит доверие к автоматизированным системам.

Литература

Актуальные киберугрозы для организаций: итоги 2023 года. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/

Артамонов В. А., Артамонова Е. В., Сафонов А. Г. Кибернетические и информационные войны: основные вызовы и игроки. СПб., 2022.

Будылина Е. И. Возможности выявления признаков личности человека по его цифровой личности / Юридические исследования. – 2024. – №. 8. – С. 82-93.

Вьет Н. Т., Кравец А. Г. Новый метод прогнозирования технологических трендов на основе анализа научных статей и патентов / International Journal of Open Information Technologies. – Vol. 10, № 10. – 2022. – С. 49-62.

Захаров В. П., Азарова И. В. Параметризация специальных корпусов текстов / Структурная и прикладная лингвистика. – 2012. – №. 9. – С. 176-184.

Косова М. В. Параметризация текстов документов как способ жанровой идентификации / Вестник Балтийского федерального университета им. И. Канта. Серия: Филология, педагогика, психология. – 2020. – №. 1. – С. 48-55.

Кочеткова В. Д. Патентоведческая экспертиза как инструмент защиты интеллектуальных прав / Интеллектуальная собственность как базовое условие обеспечения технологического суверенитета Российской Федерации. Сборник докладов XXVI Международной научно-практической конференции Роспатента. – 2022. – С. 35-38.

Малянова К. П. Особенности осуществления оперативно-розыскной деятельности и основные угрозы безопасности киберпространства в условиях цифровизации общества и виртуализации реальности / Сибирские уголовно-процессуальные и криминалистические чтения. – 2023. – № 2(40). – С. 87-93.

Патент RU 177377 U1, 2018. URL: https://patents.s3.yandex.net/RU177377U1_20180219.pdf

Патент RU 2256223 C2, 2005. URL: https://patents.s3.yandex.net/RU2256223C2_20050710.pdf

Патент RU 2469389 C1, 2012. URL: https://patents.s3.yandex.net/RU2469389C1_20121210.pdf

Патент RU 2559725 C1, 2015. URL: https://patents.s3.yandex.net/RU2559725C1_20150810.pdf

Патент RU 2580027 C1, 2016. URL: https://patents.s3.yandex.net/RU2580027C1_20160410.pdf

Патент RU 2634180 C1, 2017. URL: https://patents.s3.yandex.net/RU2634180C1_20171024.pdf

Патент RU 2658165 C2, 2018. URL: https://patents.s3.yandex.net/RU2658165C2_20180619.pdf

Патент RU 2701990 C1, 2019. URL: https://patents.s3.yandex.net/RU2701990C1_20191002.pdf

Патент RU 2719553 C1, 2020. URL: https://patents.s3.yandex.net/RU2719553C1_20200421.pdf

Патент RU 2780046 C1, 2022. URL: https://patentimages.storage.googleapis.com/91/f7/84/d5bf567392e8a3/RU2780046C1.pdf

Патент RU 2790330 C2, 2023. URL: https://patents.s3.yandex.net/RU2790330C2_20230216.pdf

Патент RU 2790946 C1, 2023. URL: https://patents.s3.yandex.net/RU2790946C1_20230228.pdf

Патент WO/2014/163524, 2014. URL: https://patentscope.wipo.int/search/ru/detail.jsf?docId=WO2014163524

Патент WO/2018/124931, 2018. URL: https://patentscope.wipo.int/search/ru/detail.jsf?docId=WO2018124931

Патент WO/2020/176003, 2020. URL: https://patentscope.wipo.int/search/ru/detail.jsf?docId=WO2020176003

Платформа. Викисловарь. URL: https://ru.wiktionary.org/wiki/платформа

Пристанскков В. Д., Харатишвили А. Г., Евстратова Ю. А. Искусственный интеллект–новая форма использования специальных знаний в расследовании и раскрытии киберпреступлений / Всероссийский криминологический журнал. – 2023. – Т. 17. – №. 6. – С. 586-596.

Роспатент. URL: https://searchplatform.rospatent.gov.ru/

Свиридов Д. А. Цифровой след и его значение в практике расследования преступлений / Правовая культура в современном обществе. Сборник научных статей VI Международной научно-практической конференции. – 2023. – С. 260-263.
Техники и тактики киберпреступников. Ростелеком-Солар. URL: https://rt-solar.ru/analytics/reports/3416/
Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/
PATENTSCOPE. URL: https://www.wipo.int/ru/web/patentscope.

References

Artamonov, V. A., Artamonova, E. V., Safonov, A. G. (2022). Cybernetic and information wars: main challenges and players. St. Petersburg (in Russian).
Budylina, E. I. (2024). The possibility of identifying signs of a person's personality by his digital identity. Legal Studies, 8, 82-93 (in Russian).
Current Cyber Threats for Organizations: 2023 Results. Positive Technologies. Available from: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-dlya-organizacij-itogi-2023-goda/ (in Russian).
Federal Law "On Personal Data" dated July 27, 2006. Available from: https://www.consultant.ru/document/cons_doc_LAW_61801/ (in Russian).
Kochetkova, V. D. (2022). Patent examination as a tool for protecting intellectual rights. In Intellectual property as a basic condition for ensuring the technological sovereignty of the Russian Federation. Proceedings of the XXVI International scientific and practical conference of Rospatent, 35-38 (in Russian).
Kosova, M. V. (2020). Parameterization of document texts as a method of genre identification. IKBFU's Vestnik. Series: Philology, Pedagogy, Psychology, 1, 48-55 (in Russian).
Malyanova, K. P. (2023). Features of the implementation of operational-search activities and the main threats to the security of cyberspace in the context of digitalization of society and virtualization of reality. Siberian criminal procedure and criminalistic readings, 2 (40), 87-93 (in Russian).
Patent RU 177377 U1, 2018. Available from: https://patents.s3.yandex.net/RU177377U1_20180219.pdf (in Russian).
Patent RU 2256223 C2, 2005. Available from: https://patents.s3.yandex.net/RU2256223C2_20050710.pdf (in Russian).
Patent RU 2469389 C1, 2012. Available from: https://patents.s3.yandex.net/RU2469389C1_20121210.pdf (in Russian).
Patent RU 2559725 C1, 2015. Available from: https://patents.s3.yandex.net/RU2559725C1_20150810.pdf (in Russian).
Patent RU 2580027 C1, 2016. Available from: https://patents.s3.yandex.net/RU2580027C1_20160410.pdf (in Russian).
Patent RU 2634180 C1, 2017. Available from: https://patents.s3.yandex.net/RU2634180C1_20171024.pdf (in Russian).
Patent RU 2658165 C2, 2018. Available from: https://patents.s3.yandex.net/RU2658165C2_20180619.pdf (in Russian).
Patent RU 2701990 C1, 2019. Available from: https://patents.s3.yandex.net/RU2701990C1_20191002.pdf (in Russian).
Patent RU 2719553 C1, 2020. Available from: https://patents.s3.yandex.net/RU2719553C1_20200421.pdf (in Russian).
Patent RU 2780046 C1, 2022. Available from: https://patentimages.storage.googleapis.com/91/f7/84/d5bf567392e8a3/RU2780046C1.pdf (in Russian).
Patent RU 2790330 C2, 2023. Available from: https://patents.s3.yandex.net/RU2790330C2_20230216.pdf (in Russian).
Patent RU 2790946 C1, 2023. Available from: https://patents.s3.yandex.net/RU2790946C1_20230228.pdf (in Russian).
Patent WO/2014/163524, 2014. Available from: https://patentscope.wipo.int/search/ru/detail.jsf?docId=WO2014163524 (in Russian).
Patent WO/2018/124931, 2018. Available from: https://patentscope.wipo.int/search/ru/detail.jsf?docId=WO2018124931 (in Russian).
Patent WO/2020/176003, 2020. Available from: https://patentscope.wipo.int/search/ru/detail.jsf?docId=WO2020176003 (in Russian).
PATENTSCOPE. Available from: https://www.wipo.int/ru/web/patentscope (in Russian).
Platform. Wiktionary. Available from: https://ru.wiktionary.org/wiki/платформа (in Russian).
Pristanskov, V. D., Kharatishvili, A. G., Evstratova, Ju. A. (2023). Artificial Intelligence – a New Form of Using Special Knowledge in Investigating and Solving Cybercrimes. Russian Journal of Criminology, 17(6), 586-596 (in Russian).
Rospatent. Available from: https://searchplatform.rospatent.gov.ru/ (in Russian).
Sviridov, D. A. (2023). Digital trace and its importance in the practice of crime investigation. In Legal culture in modern society. Proceedings of the VI International scientific and practical conference, 260-263 (in Russian).
Techniques and tactics of cybercriminals. Rostelecom-Solar. Available from: https://rt-solar.ru/analytics/reports/3416/ (in Russian).
Viet, N. T., Kravets, A. G. (2022). A new method for predicting technological trends based on the analysis of scientific articles and patents. International Journal of Open Information Technologies, 10(10), 49-62 (in Russian).
Zakharov, V. P., Azarova, I. V. (2012). Parameterization of special text corpora. Structural and Applied Linguistics, 9, 176-184 (in Russian).

Citation:
Мамаев И. Д., Марусенко М. А., Петров В. В. Цифровые социальные угрозы: от лингвистики до криминалистики в зеркале патентных решений // Юрислингвистика. – 2025 – 36. – С. 74-81.

Mamaev I. D., Marusenko M. A., Petrov V. V. (2025) Digital Social Threats: From Linguistics to Forensic Science in the Mirror of Patent Solutions. Legal Linguistics, 36, 74-81.