

Оригинальная статья / Original article
<https://doi.org/10.31429/20785836-13-4-55-63>



ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ СБОРА И АНАЛИЗА ДОКАЗАТЕЛЬСТВ

Р.И. Дремлюга*, А.И. Коробеев

ФГАОУ ВО «Дальневосточный федеральный университет»
(п. Аякс, 10, о. Русский, г. Владивосток, Приморский край, Россия, 690922)

Ссылка для цитирования: Дремлюга Р.И., Коробеев А.И. Применение искусственного интеллекта для сбора и анализа доказательств. *Юридический вестник Кубанского государственного университета*. 2021;13(4):55–63. <https://doi.org/10.31429/20785836-13-4-55-63>

КОНТАКТНАЯ ИНФОРМАЦИЯ:

Дремлюга Роман Игоревич, кандидат юридических наук, заместитель директора Юридической школы по развитию, руководитель программы «Искусственный интеллект и большие данные» Института математики и компьютерных технологий

Адрес: п. Аякс, 10, о. Русский, г. Владивосток, Приморский край, Россия, 690922

Тел.: + 7 (423) 265-24-24

E-mail: dremluga.ri@dvfu.ru

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Финансирование. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №18-29-16129

Статья поступила в редакцию: 18.10.2021

Статья принята к печати: 18.11.2021

Дата публикации: 29.12.2021

Аннотация: В статье исследуются существующие подходы к вопросу применения искусственного интеллекта для сбора и анализа доказательств. Решаются задачи, связанные с определением предела и требований для использования систем искусственного интеллекта в работе следствия с доказательствами. Выявляются методологические принципы их систематизации и классификации для определения перспектив применения искусственного интеллекта для сбора и анализа доказательств.

Методы: Работа опирается на требования и принципы системного анализа, а именно: объективность, всесторонность, полнота исследования. Основной метод исследования – классификация, предполагающая охват всех объектов классификационного деления и обоснование объективных оснований для их градации на виды.

Результаты: в качестве исходной позиции отмечены общие требования для использования технологии искусственного интеллекта с целью принятия решений, существенно влияющих на жизнь людей. Доказано отличие необходимых требований, предъявляемых к системам, для сбора и анализа доказательств. Признано, что одной из ключевых проблем остается обеспечение прозрачности принимаемых интеллектуальных решений и рекомендаций. В первую очередь это касается решений, основанных на использовании машинного обучения глубоких нейронных сетей. Модели машинного обучения часто очень сложны и поэтому не поддаются непосредственной проверке человеком. Для их понимания и прозрачности необходимо предусматривать специальные средства интерпретации и анализа результатов. Особо авторы отмечают, что использовать результаты работы непрозрачных систем искусственного интеллекта для сбора и анализа доказательств надо крайне осторожно, так как система не так предсказуема, как традиционные компьютерные программы.

Ключевые слова: искусственный интеллект, нейронные сети, сбор и анализ доказательств, криминалистика, уголовное право.

THE USE OF ARTIFICIAL INTELLIGENCE TO GATHER AND ANALYSE EVIDENCE

Roman I. Dremluga*, Alexander I. Korobeev

FGAOU VO "Far Eastern Federal University"

(Ayaks 10, p. Russkiy, Vladivostok, Primorsky Krai, Russia, 690922)

Link for citation: Dremluga R.I., Korobeev A.I. The use of artificial intelligence to gather and analyse evidence. *Legal Bulletin of the Kuban State University*. 2021;13(4):55–63. <https://doi.org/10.31429/20785836-13-4-55-63>

CONTACT INFORMATION:

Roman I. Dremluga, Cand. of Sci. (Law), Deputy Director of the Law School for Development, Head of the Artificial Intelligence and Big Data Master Program, Institute of Mathematics and Computer Technology

Address: Ayaks 10, p. Russkiy, Vladivostok, Primorsky Krai, Russia, 690922

Tel.: + 7 (423) 265-24-24

E-mail: dremluga.ri@dvfu.ru

Conflict of interest. The authors declare that they have no conflicts of interest.

Financing. The reported study was funded by RFBR according to the research project № 18-29-16129

The article was submitted to the editorial office: 18.10.2021

The article has been accepted for publication: 18.11.2021

Date of publication: 29.12.2021

Annotation: This article explores existing approaches to the issue of applying artificial intelligence to evidence collection and analysis. Problems associated with the definition of the limit and requirements for the use of artificial intelligence systems in the work of investigation with the evidence are solved. The methodological principles of their systematization and classification for determining the prospects of application of artificial intelligence for the collection and analysis of evidence are revealed.

Methods: The work is based on the requirements and principles of system analysis, namely: objectivity, comprehensiveness, completeness of the study. The main method of research is classification, which assumes the coverage of all objects of the classification division and the justification of objective grounds for their gradation into types.

Results: The general requirements for the use of artificial intelligence technology to make decisions that significantly affect people's lives are noted as a starting point. The differences in the necessary requirements for systems to collect and analyse evidence have been proven. It is recognised that one of the key challenges remains the transparency of intelligent decisions and recommendations. This is particularly the case with deep neural network machine learning solutions. Machine learning models are often very complex and therefore not directly verifiable by humans. In order to understand and make them transparent, special tools for interpreting and analysing results must be provided. The authors point out in particular that the results of opaque artificial intelligence systems must be used with great care in gathering and analysing evidence, as the system is not as predictable as traditional computer programs.

Keywords: artificial intelligence, neural networks, evidence collection and analysis, forensics, criminal law.

Введение

Искусственный интеллект является прорывной информационной технологией, которая имеет существенное влияние на жизнь общества уже сейчас и, судя по всему, коренным образом преобразует все социальное устройство в будущем. Логично предположить, что технология, которая так кардинально повлияет на общество, изменит и сферу борьбы с преступностью, сможет повысить выявляемость преступных деяний и упростить процесс сбора доказательств вплоть до его полной автоматизации.

Существует множество определений искусственного интеллекта. Для простоты мы будем оперировать определением зарубежных исследователей, которые понимают искусственный интеллект как способность машины (технического средства, компьютера) имитировать интеллектуальное поведение (англ. AI is the capability of a machine to imitate intelligent behavior) [16, с.

23]. Речь о поведении, до этого приписываемого только человеку, от анализа информации и поиска закономерностей до творческой деятельности.

Отдельные российские авторы подчеркивают, что «интеллектуальной называется система, способная целеустремленно, в зависимости от состояния информационных входов, изменять не только параметры функционирования, но и сам способ своего поведения, причем способ поведения зависит не только от текущего состояния информационных входов, но также и от предыдущих состояний системы» [10, с. 67]. Данное определение очерчивает один из признаков, отличающих системы искусственного интеллекта от других компьютерных систем. Интеллектуальные системы более самодетерминированы и менее зависят от входных параметров, чем другие компьютерные системы. Логично, что интеллектуальная система может анализировать информацию и находить закономерности в данных, которые связаны с совершением преступлений.

В настоящий момент жизнь людей все больше переносится в пространство виртуальное. Вместо реальных свиданий онлайн знакомства, вместо магазина из бетона и стекла страница в сети Интернет, вместо активного отдыха на природе многопользовательские компьютерные игры. Не избежала переноса в киберпространство и преступная деятельность. В сети торгуют наркотиками [5], склоняют к самоубийству, распространяют порнографические материалы и многое другое. Анализ таких объемов противоправной информации, которая публикуется в сети, в целях выявления преступлений требует огромных людских ресурсов. В свою очередь искусственный интеллект может решить данную проблему, предлагая дешевый и быстрый способ выявления и анализа огромного массива информации, публикуемой в соцсетях.

Целью данного исследования является определение пределов и систематизация применения анализа социальных сетей с помощью искусственного интеллекта для выявления преступлений и сбора доказательств. Нет сомнений, что использование данной перспективной технологии должно расширить возможности правоохранительных органов в сфере повышения эффективности установления личности преступников и привлечения их к уголовной ответственности. Однако, на наш взгляд, исследование не может быть в должной степени качественным и состоятельным в отрыве от оценки реальных возможностей технологии на данный момент и прогнозирования ее развития в ближайшем будущем.

Методы исследования

Данное исследование является результатом анализа работ российских и зарубежных авторов, посвященных применению искусственного интеллекта для выявления преступлений, сбора и анализа доказательств. Посредством обзора публикаций авторы пытаются оценить возможности современных интеллектуальных технологий в вопросе выявления противоправной деятельности и поиска доказательств в открытых электронных источниках. Анализ предпринимается и с целью выявить пределы возможного применения технологии искусственного интеллекта в данной сфере, а также риски, связанные с ее использованием.

Результаты исследования

А) Характеристики искусственного интеллекта.

В наши дни наиболее распространенным подходом для разработки систем искусственного интеллекта являются глубокие нейронные сети. Суть данного метода построения заключается в компьютерной имитации нейронных сетей живых организмов (например, головного мозга человека). Применение нейронных сетей позволяет эффективно решать задачи разного спектра – от имитации речи человека до навигации автомобиля [7, с. 7–10]. Во многих сферах искусственный интеллект уже значительно эффективней, чем человеческий мозг. Например, интеллектуальная система, разработанная компанией Google, обыграла нескольких чемпионов по азиатским шашкам Го. Долгое время считалось, что превосходство компьютера в этой сфере недостижимо, так как данный вид настольной игры невозможно просчитать¹. Стоит отметить, что систему научили выигрывать не программисты, а она сама научилась играть на таком превосходном уровне, тренируясь играть против самой себя. Для того, чтобы играть лучше людей-чемпионов искусственный интеллект сыграл 29 млн тренировочных партий [17].

Традиционная ошибка, которая тиражируется в современной юридической литературе, сводится к неправильному пониманию процесса создания систем искусственного интеллекта. Системы, основанные на искусственных нейронных сетях (а их сейчас большинство), не программируются, а обучаются. Для тренировки искусственного интеллекта нужны либо большие объемы данных, либо взаимодействие с системами, которые генерируют данные. Разработчик в этом

¹ Количество комбинаций в данной игре больше, чем атомов во вселенной

случае не определяет все возможные варианты поведения системы, а лишь проектирует архитектуру и проверяет соответствие работы системы после обучения заданным целям. Предсказать, как будет вести себя система, можно лишь с определенной долей вероятности. Неправильное понимание процесса создания и характеристик работы систем искусственного интеллекта ведет к затруднению во внедрении систем искусственного интеллекта в правоохранительную деятельность.

Например, некоторые российские исследователи считают, что алгоритм действий робота создается человеком, даже если речь идет об искусственном интеллекте и самообучаемых нейронных сетях [3, с. 51]. Другие же считают, что важнейшим вопросом использования интеллектуальных компьютерных систем является правовая регламентация «вопроса об ошибках при программировании и их последствиях» [4, с. 17].

В рамках нашего исследования мы выделяем два основных отличия систем искусственного интеллекта от традиционных компьютерных систем: автономность и непрозрачность.

Как справедливо отмечают некоторые исследователи, существенно значимыми характеристиками автономности являются:

- субъектность (в том числе – автономность как интеллектуального агента, самостоятельность и самореферентность в самообучении и в выработке и принятии решений);
- когнитивная и адаптационная автономность;
- пространственно-кинетическая автономность (речь об аппаратной автономности и возможности физически воздействовать на окружающий мир);
- автономность программно-энергетического управления (в том числе самостоятельность в само-включении-отключении-перезапуске и возможность воспрепятствования внешнему отключению);
- энергетическая автономность [8, с. 105].

Таким образом, автономность означает, что, хотя бы де-факто центром принятия решений становится система искусственного интеллекта. Системы сами способны анализировать информацию, классифицировать данные, принимать решения (в зависимости от ситуации) автономно от человека. Примером типичной задачи классификации данных является выявление возможных подозреваемых на месте преступления. Система, имея данные о времени, месте и типе преступления, пользуясь информацией с камер наблюдения выдает суждения о возможных подозреваемых [11]. Это не означает, что такая криминалистическая работа полностью избавляет правоохранительные органы от проведения подобных действий. Тем не менее применение системы искусственного интеллекта экономит ресурсы и повышает эффективность такой работы. То есть автономность ИИ не означает, что вмешательства человека не требуется вообще, но умные системы способны проделывать значительную часть интеллектуальной работы без участия человека.

Серьезным ограничением для использования интеллектуальных систем правоохранительными органами является их непрозрачность. Это свойство характерно для большинства современных систем искусственного интеллекта, использующих глубокие нейронные сети. Непрозрачность можно понимать в нескольких смыслах. Во-первых, непрозрачность на основании закона, когда речь идет о коэффициенте нейронной сети или ее архитектуры в связи тем, что это интеллектуальная собственность компании или государственная тайна [12, с. 3].

Второй вариант непрозрачности интеллектуальных систем вызван тем, что понимание принципов работы систем искусственного интеллекта – это специализированный навык, недоступный для большинства людей. Необходимо изучать синтаксис языков программирования, чтобы понимать компьютерные программы [12, с. 4]. С архитектурой современных систем искусственного интеллекта, например, нейронных сетей, все еще сложнее. Для понимания работы ИИ требуются как глубокие математические знания, так и погружение в компьютерные методы анализа данных [7, с. 38].

Третий вид непрозрачности в некотором смысле непреодолим. Современные системы искусственного интеллекта настолько сложны, что практически недостижимы для человеческого понимания. Например, система искусственного интеллекта может оперировать триллионами единиц данных в тысячемерном пространстве [12, с. 4]. Специалист в лучшем случае сможет понять основные характеристики работы системы, но никогда не предскажет результаты ее работы в каждом конкретном случае.

Современные системы ИИ, как правило, очень сложны и в основном не способны объяснить, как и почему они пришли к такому решению. Без этих знаний и обоснований доказательство соответствия криминалистическим стандартам практически невозможно. Чтобы сократить время криминалистической экспертизы, осуществляемой с помощью ИИ (прежде всего глубоких

нейронных сетей), необходимо использовать специальные модели визуализации и объяснения решений. К сожалению, несмотря на значительные прорывы в этой области, большинство систем не соответствует критериям необходимой «прозрачности». Прозрачность, по сути, – это возможность получить доступ к логике, лежащей в основе решения, принятого обученной для решения каких-то задач системой ИИ [15].

Таким образом, для выявления преступлений и сбора доказательств должны использоваться только понятные системы, логика решений которых прозрачна для специалистов. В противном случае использовать непрозрачные системы в криминалистической сфере не представляется возможным. Использование систем, логику которых мы не понимаем, будет сродни тому, как если бы мы использовали для определения подозреваемых гадание на кофейной гуще.

Одним из самых распространенных рисков, упоминаемых в научной литературе, который связан с использованием непрозрачных систем ИИ в правоохранительной деятельности, является маргинализация каких-либо групп людей. В сфере уголовного правосудия необъективный вывод, приводящий к дискриминационному эффекту, может нанести серьезный ущерб вовлеченным лицам. Так, в США независимыми экспертами было доказано, что запатентованный алгоритм под названием COMPAS, используемый при принятии решений об освобождении под залог, дал результат, который был предвзятым по отношению к чернокожим обвиняемым несмотря на то, что раса не использовалась в качестве предиктора [13]. При этом непрозрачная система использовалась на протяжении почти десятилетия до того, как был обнаружен ее существенный недостаток. Таким образом, существует риск, что такие системы будут направлены прежде всего против людей, которые стереотипно воспринимаются обществом как преступные элементы. Скажем, это могут быть какие-либо национальности или профессии.

Б) Необходимые качества системы ИИ, используемой для сбора и анализа доказательств.

Для того чтобы избежать вышеупомянутого и других рисков, связанных с системами ИИ, которые используются в уголовном процессе, алгоритм должен обладать следующими свойствами: консультативный характер; законность использования данных; детализация данных; возможность оспаривания; точность; ответственность; объяснимость [14].

Консультативный характер подразумевает, что программа является лишь консультантом сотруднику правоохранительных органов, который является истинным центром принятия решений. При этом необходимо удостовериться, что использование ИИ не подразумевает простую легализацию его решений человеком. И человек из крови и плоти осознано принимает или не принимает совет, предложенный системой.

Законность означает, что данные, используемые для принятия решений системой ИИ, максимально не персонализированы. Также это подразумевает, что вмешательство в личную жизнь людей пропорционально рискам, которые устраняются с помощью такого вмешательства. Так, для выявления лиц, разбрасывающих мусор на улице, будет не пропорционально получать доступ ко всем финансовым данным или данным о перемещении таких лиц за месяц.

Детализация данных подразумевает, что мы знаем, каким образом получены данные для обучения нашей системы ИИ. Мы должны также понимать характеристики этих данных, их охват и представительность. Кроме того, необходимо понимать, кто работал и как получил данные, используемые для принятия решения.

Возможность оспаривания подразумевает, что любой вывод, сделанный системой искусственного интеллекта, может быть оспорен. Кроме того, должна быть доступна вероятностная оценка принятого решения. Например, решение ИИ может быть принято на пороге допустимой вероятности его правильности, такое решение обладает меньшей степенью достоверности и применимости при анализе и сборе доказательств.

Точность как характеристика ИИ означает долю правильных ответов, которые дает система. Точность должна регулярно подвергаться переоценке, так как с течением времени данные, которые поступают для принятия решений системой, могут значительно отличаться, от тех, на которых система училась. Например, если мы разработали систему, которая определяет возраст человека, написавшего текст, со временем стиль письма и характерные выражения для разного возраста могут меняться, поэтому точность модели должна уменьшиться.

Ответственность использования подразумевает соответствие общественным интересам и этическим нормам. Использование системы должно оцениваться не только с точки зрения технических характеристик, но и ее влияния на общество. В случае с оценкой и анализом доказательств посредством ИИ при неправильном использовании или ошибке в алгоритме

последствия могут быть катастрофическими. Поэтому правоохранительным органам следует применять интеллектуальную систему, осознавая все риски такого применения для общества.

Пожалуй, самая главная характеристика систем искусственного интеллекта для сбора и анализа доказательств – это объяснимость. Без объяснения того, как было получено или выделено отдельное доказательство или их группа, невозможно их использование в уголовном процессе. Зачастую вопросы к системам ИИ формулируются таким же образом, как и к экспертам-криминалистам, следовательно, система должна предоставлять степень объяснимости не ниже, чем это происходит при работе экспертов.

Существуют первые нормативные документы, которые определяют требования к системам ИИ, используемым в судебной сфере. Так, европейской комиссией по эффективности правосудия Совета Европы была принята Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях [6]. Хартия выделяет пять ключевых требований, которые предъявляются к использованию систем искусственного интеллекта в судебных системах и окружающих их реалиях.

Принцип уважения основополагающих прав означает соблюдение основных прав и неприкосновенность основных свобод, закрепленных в нормативных документах Совета Европы. Данный принцип касается как разработчика, так и пользователя ИИ в судебных системах.

Принцип недискриминации подразумевает, что дискриминация посредством интеллектуальных систем недопустима. Это относится как к дискриминации определенных групп, так и отдельных лиц.

Принцип качества и безопасности предполагает, что должны использоваться только проверенные и сертифицированные системы и источники данных, которые отвечают стандартам безопасности технологических продуктов.

Принцип прозрачности, беспристрастности и достоверности сводится к тому, что используемые технологии должны быть понятными и доступными для внешнего наблюдателя. Кроме того, необходимо регулярное проведение внешнего аудита и обеспечение общественного контроля результатов работы системы. Аудит также необходим для понимания актуальности предлагаемых интеллектуальной системой решений. Социальная реальность может меняться катастрофически быстро, а значит система, обучавшаяся на старых данных, будет давать результаты, нерелевантные действительности.

Принцип контроля пользователем означает, что необходимо избегать простого автоматического применения рекомендаций и решений, предлагаемых искусственным интеллектом. Пользователю следует быть информированным о характере решения и нести ответственность за его применение. В контексте деятельности по сбору и анализу доказательств данный принцип имеет ключевое значение, так как от рекомендации или решения, предлагаемых системой, может зависеть свобода невиновного лица или возможность привлечения к ответственности действительного преступника.

В) Использование систем искусственного интеллекта для сбора и анализа доказательств.

Искусственный интеллект может быть использован во многих сферах криминалистики. Так, по мнению некоторых исследователей, системы, в основе которых используются глубокие нейронные сети могут применяться в следующих частных и общих направлениях:

1. Оценка исходной информации по уголовному делу в целях выдвижения простых и комплексных следственных версий, определения направлений их проверки.

2. Моделирование события преступления и его следовой картины на основе неполных данных и предшествующего «опыта», охватывающего большой массив уголовных дел.

3. Выявление признаков серийности в условиях информационной недостаточности и предложение вариантов действий следователя по проверке перспективных следственных версий.

4. Увеличение эффективности почерковедческих и габитоскопических исследований (например, автоматизация выявления признаков подлога документов).

5. Поиск недоступных криминалистическому программному обеспечению компьютерных файлов, сокрытых, например, при помощи стеганографии или альтернативных потоков данных, установление первичного источника информации в сети Интернет.

6. Дополнительная оценка достаточности собранных доказательств для предъявления обвинения или направления уголовного дела прокурору.

7. Прогнозирование совершения преступления в будущем на основе анализа признаков совершенных преступлений с точки зрения их локализации, социальных характеристик участвующих лиц, средств массовой информации.

8. Стратегическое планирование, к примеру построение логических моделей [1, с. 46].

Лучше всего ИИ, основанные на нейронных сетях, ищут скрытые закономерности на больших массивах данных. Поиск взаимосвязей на больших объемах информации недоступен человеку без применения математических методов. Так, в результате одного из исследований искусственный интеллект был применен к анализу серийных преступлений. В результате использования методов ИИ были выявлены типичные признаки преступлений и закономерные связи между ними. Обученные учеными интеллектуальные системы поддержки принятия решений дали возможность прогнозировать с высокой точностью расстояние от места преступления до места жительства преступника, возраст преступника, наличие у него психического заболевания и судимости, а также некоторые другие характеристики [2].

В рамках другого исследования было доказано, что искусственный интеллект необходим для использования в работе следователя. Это позволяет повысить его эффективность, решить проблему нехватки квалифицированных кадров для органов следствия, а также увеличить долю раскрываемости преступлений. В настоящий момент количество данных, накопленных в рамках следственной работы, достигло того значения, когда можно эффективно обучать нейронные сети и использовать другие методы ИИ [9].

Научная дискуссия

Один из наиболее дискуссионных вопросов, который возникает в связи с достижениями в сфере использования искусственного интеллекта, заключается в готовности применять полученные знания для сбора и анализа доказательств. Несмотря на то, что ИИ перспективен для внедрения практически в любой сфере, в рассматриваемом случае остается открытым ряд вопросов.

Одной из ключевых проблем является обеспечение прозрачности принимаемых интеллектуальных решений и рекомендаций. В первую очередь это касается решений, основанных на использовании машинного обучения глубоких нейронных сетей. Традиционная разработка программного обеспечения, система которой складывалась годами, следует определенному «жизненному циклу». Он начинается с определения требований, проходит через проектирование к реализации, например, кодированию, а затем программное обеспечение постепенно тестируется по мере интеграции отдельных частей программного обеспечения в общую систему. Там, где системы являются критически важными, требования к этапам жизненного цикла очень строгие и прозрачные. Ключевые требования, например, к безопасности, определяются и уточняются на каждом этапе разработки. Также проводится стандартизированное тестирование, которое охватывает необходимые диапазоны входных данных. Как правило, при наличии официальной системы регулирования стандарты определяют, что необходимо сделать для достижения уверенности и получения разрешения на развертывание системы.

В отличие от этого, разработка систем на основе нейронных сетей является весьма итеративным процессом, с совершенно иным жизненным циклом, и существующие стандарты не дают основы для обеспечения гарантий. Модели, лежащие в основе систем машинного обучения, обучаются на данных, представляющих проблему, которую необходимо решить, а затем их производительность оценивается по заранее заданным критериям и совершенствуется до тех пор, пока их производительность не станет удовлетворительной. Эти модели полезны, поскольку они обобщают данные, полученные в ходе начального обучения. Например, автономные транспортные средства могут идентифицировать пешеходов в ситуациях, которых не было в наборе данных для обучения, предсказывать их траекторию и выполнять маневры, чтобы избежать столкновения. То есть работать на данных реального мира, а не заданного набора.

Модели машинного обучения часто очень сложны и поэтому не поддаются непосредственной проверке человеком («непрозрачная модель» или «черный ящик»). Кроме того, структура модели машинного обучения может не соответствовать характеристикам, которые человек использовал бы при принятии решений, поэтому интерпретация останется сложной, даже если бы модель можно было проверить. Некоторые системы анализа изображений могут ошибочно классифицировать объекты, когда добавляется небольшое количество шума, незаметного для человека, но очень значимого в модели из-за особенностей обучения.

Непрозрачность автоматически означает, что использовать результаты работы систем искусственного интеллекта для сбора и анализа доказательств надо крайне осторожно, так как система не так предсказуема, как традиционные компьютерные программы. Необходимо прилагать дополнительные усилия, чтобы сделать логику работы программы прозрачной для пользователя и лиц, на чью жизнь влияют полученные результаты. Любая система, которая используется в рамках следствия по уголовному делу, должна быть доступна для внешнего аудита своей работы.

Заклучение

Применение искусственного интеллекта для сбора и анализа доказательств – вопрос достаточно новый. Технология, как и опыт ее применения, только начинают складываться. На этом этапе развития рано говорить о применимости или неприменимости систем искусственного интеллекта для сбора и анализа доказательств. В нашем научном обзоре мы попытались очертить рамки и требования для использования таких систем. Основным препятствием для использования ИИ при этом является непрозрачность его работы и полученных решений, что затрудняет его применение в деятельности следственных органов, но не исключает полностью.

Список использованной литературы:

1. Бахтеев Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования. *Российское право: образование, практика, наука*. 2018;(2):43–49.
2. Бессонов А.А. Использование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений). *Вестник Университета имени О.Е. Кутафина (МГЮА)*. 2021;(2):45–53.
3. Васильев А.А., Ибрагимов Ж.И. Правовое регулирование робототехники и искусственного интеллекта в европейском союзе. *Российско-азиатский правовой журнал*. 2019;(1):50–54.
4. Васильев А.А., Печатнова Ю.В. Искусственный интеллект и право: проблемы, перспективы. *Российско-азиатский правовой журнал*. 2020;(2):14–18.
5. Дремлюга Р.И. Незаконный оборот наркотиков и крипторынки: угрозы и вызовы правоохранителю. *Наркоконтроль*. 2018;(2):33–38.
6. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. СПб.: Питер, 2020.
7. Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права. *Вестник Российского университета дружбы народов. Серия: Юридические науки*. 2018;22(1):91–109.
8. Сибилькова А.В. Искусственный интеллект на службе у следователя. *Российский следователь*. 2019;(3):68–70.
9. Якушев Д.И. Об определении искусственного интеллекта // *В сборнике: Региональная информатика и информационная безопасность. Сборник трудов*. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления; 2016. С. 67–69.
10. AL-Marghilani A.A. Target Detection Algorithm in Crime Recognition Using Artificial Intelligence. *CMC-Computers, Materials & Continua*. 2021;71(1):809–824.
11. Burrell J. How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. *Big Data & Society*. January–June, 2016.
12. Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner "Machine Bias". *ProPublica*. May 23, 2016. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
13. Marion Oswald, Jamie Grace, Sheena Urwin & Geoffrey C. Barnes Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality. *Information & Communications Technology Law*. 2018. Pp. 223–250.

References:

1. Bahteev D.V. [Artificial Intelligence in Criminalistics: Status and Prospects of Use]. *Rossiiskoe pravo: obrazovanie, praktika, nauka = Russian law: education, practice, science*. 2018;(2):43–49. (In Russ.)]
2. Bessonov A.A. [The use of artificial intelligence algorithms in the criminalistic study of criminal activity (on the example of serial crimes)]. *Vestnik Universiteta imeni O.E. Kutafina (MGYUA) = Bulletin of O.E. Kutafin University (MSUA)*. 2021;(2):45–53. (In Russ.)]
3. Vasil'ev A.A., Ibragimov ZH.I. [Legal regulation of robotics and artificial intelligence in the European Union]. *Rossiisko-aziatskij pravovoj zhurnal = Russian-Asian Legal Journal*. 2019;(1):50–54. (In Russ.)]
4. Vasil'ev A.A., Pechatnova YU.V. [Artificial intelligence and law: problems, prospects]. *Rossiisko-aziatskij pravovoj zhurnal = Russian-Asian Legal Journal*. 2020;(2):14–18. (In Russ.)]
5. Dremlyuga R.I. [Drug trafficking and crypto markets: threats and challenges to law enforcement]. *Narkokontrol' = Drug Control*. 2018;(2):33–38. (In Russ.)]
6. Nikolenko S., Kadurin A., Arhangel'skaya E. [Deep Learning]. SPb: Peter, 2020. (In Russ.)]
7. Ponkin I.V., Red'kina A.I. [Artificial intelligence from the point of view of law]. *Vestnik Rossijskogo universiteta druzhby narodov. Seriya: YUridicheskie nauki = Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences*. 2018;22(1):91–109. (In Russ.)]
8. Sibil'kova A.V. [Artificial intelligence in the service of the investigator]. *Rossiiskij sledovatel' = A Russian investigator*. 2019;(3):68–70. (In Russ.)]
9. Yakushev D.I. [About the definition of artificial intelligence]. *In the collection: Regional Informatics and information security. Collection of works*. St. Petersburg Society of Informatics, Computer Technology, Communication and Control Systems; 2016. Pp. 67–69. (In Russ.)]
10. AL-Marghilani A.A. Target Detection Algorithm in Crime Recognition Using Artificial Intelligence. *CMC-Computers, Materials & Continua*. 2021;71(1):809–824.
11. Burrell J. How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. *Big Data & Society*. January–June, 2016.
12. Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner "Machine Bias". *ProPublica*. May 23, 2016. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
13. Marion Oswald, Jamie Grace, Sheena Urwin & Geoffrey C. Barnes Algorithmic risk assessment policing models: lessons from the Durham HART model and "Experimental" proportionality. *Information & Communications Technology Law*. 2018. Pp. 223–250.

DOI: 10.1080/13600834.2018.1458455

14. Minarcin M. Building Responsibility in AI: Transparent AI for Highly Automated Vehicle Systems. *SAE Technical Papers*. 2021.

DOI: <https://doi.org/10.4271/2021-01-0195>

15. Padhy N.P. Artificial intelligence and intelligent systems 3. Oxford University Press, 2005. Pp. 23.

16. Silver D., Schrittwieser J., Simonyan K., Antonoglou I., Huang A., Guez A., Hubert T., Hassabis D. et. al. Mastering the game of Go without human knowledge. *Nature*. 2017;550(7676):354–359.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Дремлюга Роман Игоревич

кандидат юридических наук, заместитель директора Юридической школы по развитию, руководитель программы «Искусственный интеллект и большие данные» Института математики и компьютерных технологий ФГАОУ ВО «Дальневосточный федеральный университет»

ORCID: <https://orcid.org/0000-0003-1607-1228>

Author ID: 56622488500

Web of Science Researcher ID U-9979-2019

Коробеев Александр Иванович

доктор юридических наук, профессор, заслуженный деятель науки РФ, заведующий кафедрой уголовного права и криминологии Юридической школы ФГАОУ ВО «Дальневосточный федеральный университет»

Author ID: 55537246800

DOI: 10.1080/13600834.2018.1458455

14. Minarcin M. Building Responsibility in AI: Transparent AI for Highly Automated Vehicle Systems. *SAE Technical Papers*. 2021.

DOI: <https://doi.org/10.4271/2021-01-0195>

15. Padhy N.P. Artificial intelligence and intelligent systems 3. Oxford University Press, 2005. Pp. 23.

16. Silver D., Schrittwieser J., Simonyan K., Antonoglou I., Huang A., Guez A., Hubert T., Hassabis D. et. al. Mastering the game of Go without human knowledge. *Nature*. 2017;550(7676):354–359.

INFORMATION ABOUT THE AUTHORS

Dremluga Roman Igorevich

Cand. of Sci. (Law), Deputy Director of the Law School for Development, Head of the Artificial Intelligence and Big Data Master Program, Institute of Mathematics and Computer Technology FGAOU VO "Far Eastern Federal University"

ORCID: <https://orcid.org/0000-0003-1607-1228>

Author ID: 56622488500

Web of Science Researcher ID U-9979-2019

Korobeev Alexander Ivanovich

Dr. of Sci. (Law), Head of the Department of Criminal Law and Criminology of the Law School FGAOU VO "Far Eastern Federal University"

Author ID: 55537246800