

DOI 10.24412/2227-7315-2022-4-162-172

УДК 343.9

И.Б. Воробьева

## ЭТИЧЕСКИЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

**Введение:** появление систем искусственного интеллекта заставляет задуматься об этических аспектах их применения в процессе расследования преступлений. **Цель:** аналитическая — обозначить этические риски, возникающие при разработке систем; рекомендательная — с позиции этики дать рекомендации по использованию систем в процессе расследования. **Методологическая основа:** методы формальной и диалектической логики; методы сравнения, описания, интерпретации и др. **Результаты:** установлено, что системы искусственного интеллекта не лишены недостатков, в том числе сопряженных с этическими рисками. Нарушения этики могут быть заложены в процессе разработки систем, а также возникать в процессе использования их субъектами расследования. Содержатся рекомендации по работе субъекта расследования с данными, полученными с помощью систем искусственного интеллекта. **Выводы:** этические риски, возникающие при создании и использовании систем искусственного интеллекта, должны быть учтены при расследовании преступлений. Умение работать с такими системами является важным фактором эффективной деятельности не только субъектов расследования, но и правоохранительной системы в целом.

**Ключевые слова:** этика, этические принципы, этика искусственного интеллекта, искусственная нейронная сеть, прозрачность, достоверность, расследование преступлений.

I.B. Vorobyova

## ETHICAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS IN CRIME INVESTIGATION

**Background:** the emergence of artificial intelligence systems forces us to think about the ethical aspects of their use in the investigation of crimes. emergence of the artificial intellect systems tends to bring about some thoughts relevant to the ethical aspects of their application for criminal investigation. **Objective:** analytical — to outline the ethical risks arising in the development of systems; recommendatory — from an ethical perspective to give recommendations for the use of systems in the process of investigation. **Methodology:** methods of formal and dialectical logic; methods of comparison, description, interpretation, etc. **Results:** it has been founded that artificial intelligence systems are not without flaws, including those associated with ethical risks. Ethical violations may be inherent in the design of systems, as well as arise during their use by the subjects of the investigation. Recommendations on the work of the subject of investigation with the data obtained with the help of artificial intelligence systems are given. **Conclusions:**

---

© Воробьева Ирина Борисовна, 2022

Кандидат юридических наук, доцент кафедры криминалистики (Саратовская государственная юридическая академия); e-mail: irinavorobyeva@yandex.ru

© Vorobyova Irina Borisovna, 2022

Candidate of Law, Associate Professor, Criminalistics Department, (Saratov State Law Academy)

*ethical risks arising from the creation and use of artificial intelligence systems must be taken into account in the investigation of crimes. The ability to work with such systems is an important factor in the effective activity of not only the subjects of the investigation, but also law enforcement system as a whole.*

**Key-words:** *ethics, ethical principles, artificial intellect ethics, artificial neural network, transparency, reliability, criminal investigation.*

Достижениями в сфере информационных технологий пользуются представители практически всех сфер человеческой деятельности. Правительства и ученые многих стран<sup>1</sup> понимают, что внедрение систем искусственного интеллекта (далее — ИИ) дает серьезные поводы для обсуждения этических проблем, возникающих в связи с этим процессом, и предприняли попытки выработать этические нормы по применению систем ИИ.

В России также считают, что развитие и внедрение систем ИИ неизбежно связано с созданием соответствующих этических норм. Так, целесообразность выработки и закрепления этических норм в области обработки информации регламентирована в «Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.» Данный документ в качестве одной из ключевых целей определил формирование кодексов этических правил<sup>2</sup>. В Национальной стратегии развития искусственного интеллекта на период до 2030 года<sup>3</sup> отмечается, что проводятся научные исследования, целью которых является прогнозирование этических аспектов использования технологий ИИ (п. 57), и подчеркивается необходимость разработки этических правил взаимодействия человека с ИИ (п. 49 ж). Был также разработан Кодекс этики в сфере ИИ<sup>4</sup>, закладывающий общие этические принципы и стандарты поведения акторов (участников отношений в сфере ИИ) и определяющий риски и угрозы, возникающие при внедрении систем ИИ. Приоритетными направлениями развития ИИ, позволяющими минимизировать этические риски, являются: уважение фундаментальных прав личности; недо-

<sup>1</sup> Правительство Австралии создает национальную схему этики ИИ. Канада изучает этические последствия применения ИИ. Китай стремится возглавить мир в области этических норм, которые способствуют развитию ИИ. Комиссия ЕС стремится обеспечить наличие соответствующей этической и правовой базы. Германия выступает за содействие развитию прозрачного и этичного ИИ. Мексика рассматривает возможные варианты использования ИИ с учетом этики. Скандинаво-Балтийский регион призывает к разработке этических стандартов, принципов и ценностей. Швеция планирует разрабатывать правовые и этические рамки применения ИИ. Великобритания планирует изучить этические последствия достижений в области ИИ. В США сделаны конкретные рекомендации, касающиеся этики. См.: Обзор отдельных вопросов в области больших данных и искусственного интеллекта.

<sup>2</sup> См.: Распоряжение Правительства РФ от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 г.» URL: <https://legalacts.ru/doc/rasporjazhenie-pravitelstva-rf-ot-19082020-n-2129-r-ob-utverzhdanii/> (дата обращения: 21.03.2022).

<sup>3</sup> См.: Национальная стратегия развития искусственного интеллекта на период до 2030 г. утверждена Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации»). URL: <http://publication.pravo.gov.ru/Document/Text/0001201910110003> (дата обращения: 24.03.2022).

<sup>4</sup> Кодекс подготовлен совместно Аналитическим центром при Правительстве РФ, Министерством экономики и развития РФ и Альянсом в сфере искусственного интеллекта, при участии представителей государства и научного сообщества. В октябре 2021 года в рамках форума: «Этика искусственного интеллекта: начало доверия» был подписан Кодекс этики. См.: Кодекс этики в сфере искусственного интеллекта. URL: <https://berza.ru/wp-content/uploads/2021/10/kodeks-etiki-v-sfere-iskusstvennogo-intellekta.pdf> (дата обращения: 21.03.2022).

пустимость дискриминации; обеспечение качества и безопасности алгоритмов; обеспечение качества и понятности данных; прозрачность систем ИИ.

Необходимо отметить большую сложность конструирования систем ИИ с «вшитыми» в них этическими компонентами. Включение этических принципов в стандарты применения ИИ усугубляет тот факт, что сами стандарты могут существенно различаться в зависимости от государств, регионов, культурных особенностей, традиций и даже менталитета. Поскольку у принципов этики не может быть государственных границ, при разработке программ должны учитываться моральные и нравственные ценности людей по всему миру, а не только страны, откуда родом разработчик. Это особенно важно в контексте трансграничной преступности.

Нормы морали, действующие в обществе, приобретают специфику в зависимости от вида деятельности, а их соблюдение является важнейшим фактором в предотвращении нежелательных последствий. Это особенно касается процесса расследования преступлений, поскольку данная деятельность связана с вторжением в область свободы другого человека.

Основу деятельности по расследованию преступлений составляет: получение криминалистически значимой информации; анализ полученной информации и принятие решения о возможности ее использования в процессе расследования; использование полученной информации.

Значимая информация для криминалистики, по мнению Р.С. Белкина, — означает «любую информацию, используемую для решения криминалистических задач, вне зависимости от ее рода и источника» [1, с. 237]. Процесс определения значимости криминалистической информации для достижения целей расследования всегда субъективен. В условиях разнообразия современной преступности системы ИИ становятся важным ресурсом получения информации и могут быть полезны для поиска цифровых следов, выявления скрытых связей между различными объектами (людьми, мобильными телефонами, автомобилями, местами и т.п.) и т.д. Системы ИИ вполне могут выполнять функции классификатора, помогать в установлении наличия/отсутствия состава преступления, указывать на логические пробелы и коллизии в доказывании, могут рекомендовать проведение той или иной судебной экспертизы, помочь сформулировать вопросы экспертам, синтезировать доказательственную базу в обвинительное заключение и т.д. На основании информации, полученной с помощью ИИ можно выдвигать наиболее вероятные версии и определять направление расследования.

Системы ИИ можно использовать для создания различных криминалистических моделей, способствующих организации процесса расследования преступлений. Возможно создание ретроспективных моделей, что особенно важно на первоначальном этапе расследования, когда необходимо составить общее представление о фактической картине расследуемого события и выработать алгоритм расследования. Создание перспективных моделей может способствовать пресечению неправомерного и неэтичного воздействия на участников уголовного судопроизводства (например, путем анализа социальных связей участников расследуемого события). Возможно конструирование моделей поведения конкретного человека, разработка прогнозов относительно совершения преступления в определенное время и в определенном месте и тактически эффективного их пресечения. В практику правоохранительных органов уже внедрена программа, созданная на основе ИИ, позволяющая (по совокупности признаков совершенных

им преступлений) строить наиболее вероятный портрет серийного преступника<sup>1</sup>. Таким образом, использование систем ИИ, реализуемых с помощью различных устройств и приложений, может широко применяться при расследовании в сборе криминалистически значимой информации, но порождает и большое количество этических вопросов.

Информация<sup>2</sup>, устанавливаемая в процессе расследования с помощью систем ИИ должна обладать определенными свойствами: значимостью для процесса расследования; достоверностью и она должна быть получена из устойчиво функционирующих систем хранения и обработки данных.

Достоверность — одно из основных свойств, характеризующих качество информации. Она предполагает, во-первых, объективное отражение устанавливаемых фактов, явлений, процессов или деятельности; а, во-вторых, доступность для понимания и восприятия информации, содержащейся в данных, обеспечиваемая надлежащими программными и техническими средствами обработки, не приводящими к ее изменению.

Можно выделить три этапа формирования данных с помощью систем ИИ, влияющих на их достоверность: создание программ (алгоритмов); обработка данных; принятие решений на основе рекомендаций программы. Нарушения этики могут быть как изначально заложены в процессе разработки и функционирования систем ИИ, так и быть допущены непосредственно субъектом расследования в процессе работы с данными, полученными с помощью этих систем.

Рассмотрим некоторые этические риски, возникающие в процессе создания и функционирования систем ИИ. Одна из этических проблем состоит в принятии ошибочных решений на основе недостоверных данных собранных с помощью программ, основанных на ИИ. Так, например, алгоритмы, используемые для распознавания или анализа лиц, работают по-разному в зависимости от пола, возраста и этнической принадлежности идентифицируемого человека. Необходимо обратить внимание на то, что алгоритмам ИИ присущ субъективизм, поскольку они создаются, обучаются и осуществляют принятие решения на основе тех данных, которые изначально выбрал и загрузил в систему человек, или система собрала сама. Возможны ситуации, когда в базе данных, на основе которой обучаются системы ИИ, могут отсутствовать сведения, стратегически важные для принятия решения, особенно если это связано не с обычным, а экстраординарным преступлением. Уже известны случаи допущенных ошибок данными системами и их негативные последствия. Вероятны и алгоритмические ошибки, возникающие из-за использования неверных данных. Так, из-за ошибок компьютерной системы 700 сотрудников почтовой службы Великобритании отбывали тюремный срок за действия, которые они не совершали<sup>3</sup>.

Этический риск может иметь место и в случае алгоритмической предвзятости системы ИИ, которая может возникнуть как при наличии, так и отсутствии та-

<sup>1</sup> См.: Интервью руководителя НИИ криминалистики СК России А.А. Бессонова информационному агентству ТАСС. URL: <https://sledcom.ru/press/interview/item/1621439/?print=1> (дата обращения: 25.03.2022).

<sup>2</sup> Здесь и далее в том числе криминалистически значимая информация.

<sup>3</sup> См.: *Peachey K.* Post Office scandal: What the Horizon saga is all about // BBC News. URL: <https://www.bbc.com/news/business-56718036>; *Siddique H., Quinn B.* Court clears 39 post office operators convicted due to 'corrupt data' // The Guardian. URL: <https://www.theguardian.com/uk-news/2021/apr/23/court-clears-39-post-office-staff-convicted-due-to-corrupt-data> (дата обращения: 06.03.2022).



ких намерений у ее создателей. Наличие скрытых дискриминационных компонентов (расовых, гендерных, религиозных и т.д.) может привести к нарушениям прав и свобод граждан. Так, например, из-за ошибки алгоритма, созданного в США для оценки вероятности совершения преступлений, система начала проявлять признаки расизма и оценивать афроамериканцев как лиц, наиболее подверженных данному риску<sup>1</sup>. Имели место случаи, когда алгоритм занижал оценки женщин, принимаемых на работу и т.д.

Уровень этического риска, возникающего при использовании данных, полученных с помощью систем ИИ, зависит от наличия или отсутствия прозрачности алгоритмов обучения и принятия решений. Системы ИИ могут быть объяснимые (прозрачные), позволяющие легко понять действия ИИ и необъяснимые (непрозрачные). Разработчики систем не заинтересованы в раскрытии алгоритмов, поскольку они являются их интеллектуальной собственностью. Но для того, чтобы в процессе расследования объективно оценивать полученную информацию необходимо понимать, как именно конкретная программа принимает решения. Объяснительная компонента, являющаяся неотъемлемым свойством прозрачных систем ИИ, при необходимости, должна показывать ход работы системы и всю цепочку рассуждений. Например, при расследовании аварии, совершенной с участием беспилотного автомобиля и установлением её причин система должна быть настолько прозрачна, чтобы можно было проследить, на основании каких процессов сделан тот или иной вывод.

Объяснительная компонента непрозрачных систем ИИ, созданных на основе искусственных нейронных сетей методом глубокого обучения, по мнению специалистов<sup>2</sup>, представляет собой «черный ящик» и не может предъявить пользователю всю цепочку рассуждений, способствующих формированию вывода. Нельзя также быть уверенным в том, что программы, основанные на искусственных нейросетях и способные к самостоятельному извлечению информации из массива данных, в результате самообучения не создадут в дальнейшем собственный дискриминационный алгоритм. Так, стал общеизвестным факт, когда за сутки чат-бот Microsoft проявил неконтролируемое поведение и стал допускать нацистские и расистские высказывания, научился применять обесцененную лексику и писать посты порнографического характера. В итоге можно получить совершенно недостоверные данные, что является серьезным препятствием для применения информации, полученной с помощью таких систем в процессе расследования. Неслучайно в Национальной стратегии развития искусственного интеллекта на период до 2030 года отмечается, что «...Алгоритмы работы нейронных сетей крайне сложны для интерпретации, и, следовательно, результаты их работы могут быть подвергнуты сомнению и отменены человеком»<sup>3</sup>. Поэтому использование в качестве доказательств информации, полученной с помощью нейросетей, с позиции этики, является неприемлемым. Опора на данные, полу-

<sup>1</sup> См.: How We Analyzed the COMPAS Recidivism Algorithm — ProPublica. URL: <https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> (дата обращения: 27.03.2022).

<sup>2</sup> См.: Ученые: ИИ превратился в черный ящик, и с этим нужно что-то делать. URL: <https://itc.ua/blogs/uchenyie-ii-prevratilsya-v-chnyiy-yashhik-i-s-etim-nuzhno-cto-to-delat/> (дата обращения: 06.03.2022).

<sup>3</sup> Национальная стратегия развития искусственного интеллекта на период до 2030 г. (утверждена Указом Президента Российской Федерации от 10 октября 2019 г. № 490) «О развитии искусственного интеллекта в Российской Федерации». URL: <https://www.pravo.gov.ru> (дата обращения: 06.03.2022).

ченные в результате самообучения программы, может привести к выдвиганию необоснованных версий, неправильному принятию процессуального решения и выбору ошибочного направления всего процесса расследования. Вследствие этого, прежде чем использовать информацию, полученную с помощью систем ИИ в процессе расследования, необходимо выяснить механизм принятия решения конкретной программой.

Другим аспектом, влияющим на достоверность информации, является получение данных из надежно функционирующих систем хранения и обработки не приводящих к их изменению. Создаваемые программы должны обладать свойством робастности (устойчивости к внешним помехам). Отсутствие робастности может проявиться в некорректной работе программы, изменении результатов исследования, а также привести к извлечению конфиденциальных данных из обученных моделей. Не меньшей опасностью является возможность отравления (ML poisoning) машинного обучения заинтересованными лицами, т.е. манипулирование созданным алгоритмом с целью оказания влияния на принимаемые им решения. Для получения с помощью систем ИИ «...объективной криминалистически значимой информации необходимо не только их создание, но и обеспечение их защиты от многочисленных угроз путем разработки норм и правил, регламентирующих процесс создания и обработки информации» [2, с. 201].

Таким образом, условиями доверия к данным, получаемым с помощью систем ИИ, являются: использование качественных данных при создании алгоритмов; предоставление информации о механизме работы систем; соблюдение требований кибербезопасности; передача данных в доступном для понимания виде с информированием «об их сложности, точности и вероятностном интервале ошибок»<sup>1</sup>.

Как уже отмечалось, нарушения этики могут быть допущены не только со стороны систем ИИ, но и непосредственно субъектом расследования в процессе расследования. Для предотвращения этических рисков необходимо основываться на совокупности норм права, общих этических принципов, принципов и стандартов поведения участников отношений в сфере ИИ, правил и требований к служебному поведению, которыми следует руководствоваться субъекту расследования в своей профессиональной деятельности. Этика в процессе расследования преступлений сочетает в себе не только нормы права, морали, но и криминалистические рекомендации по применению систем ИИ. Если совокупность правовых норм в общих чертах регламентирует этические аспекты правовых отношений, то криминалистика разрабатывает рекомендации по этичному решению задач правоохранительными органами.

Работа с данными состоит из следующих этапов: сбор данных, содержащих значимую информацию; интерпретация полученной информации и принятии решения о возможности ее применения; хранения и использовании информации. Поскольку этические аспекты в процессе расследования приобретают особую значимость, то при работе с данными, полученными с помощью систем ИИ, следует руководствоваться здравым смыслом.

Процесс расследования неизбежно связан с проникновением в частную жизнь участников расследования, изучением их личных данных, уклада жизни, семейных отношений, заболеваний, данных об их прошлом и т.д. Принимая

<sup>1</sup>ГОСТ Р ИСО/МЭК 20546-2021 «Национальный стандарт Российской Федерации Информационные технологии. Большие данные. Обзор и словарь» (п. 4.3.5.). URL: <https://docs.cntd.ru/document/1200180276> (дата обращения: 26.03.2022).

решение о сборе и дальнейшем использовании информации важно учитывать нравственные аспекты, позволяющие предвидеть негативные последствия для участников расследования. Так, при необходимости установления причины смерти родственники потерпевшего не всегда позволяют исследовать тело умершего (по личным, религиозным или иным причинам). Такая проблема нередко возникает при необходимости вскрытия тела священнослужителя. Максимально этично помочь в установлении причины смерти без вскрытия тела позволяет криминалистическая томография или виртуальная аутопсия. Для проведения исследования тела в Швейцарии, США, Австралии уже начали применять компьютерную томографию, МСКТ (мультиспиральную компьютерную томографию) и 3D технологии<sup>1</sup>.

Недопустимо собирать информацию без наличия законных оснований, с нарушением общих этических принципов, использованием противоправных методов и, в том числе с применением технологий, используемых для обхода систем защиты данных.

При интерпретации информации важно учитывать, что алгоритмы, с помощью которых были получены данные, являются лишь продуктами человеческой деятельности и не лишены субъективизма. Поэтому не надо забывать о том, что прогнозы, сделанные с помощью алгоритмов, могут быть не всегда объективны и подвержены влиянию как человеческого фактора, так и порокам машинного обучения. Сопоставляя различные данные системы ИИ могут предлагать наиболее приемлемые алгоритмы действий, но не могут планировать, рассуждать и принимать стратегические решения. К таким данным стоит относиться с определенной долей здравого сомнения и использовать их только во вспомогательных, ориентирующих целях. Субъект расследования обязан критично оценивать полученную информацию и не должен полностью полагаться на рекомендации, предложенные программой и тем более делегировать принятие решений пусть даже самым современным системам ИИ. Критичность субъекта расследования является важнейшей нравственной основой, способствующей объективному оцениванию полученных данных и принятию решения по их дальнейшему использованию.

Следует также обратить внимание и на то, что частое обращение за помощью к своему цифровому «помощнику» чревато усугублением клиповых начал в мышлении. Такие люди испытывают трудности при анализе поступающей информации, критическом её восприятии и формулировании выводов, что влечет за собой подверженность манипуляции и ослабление эмпатии. В перспективе это может повлечь принятие типизированных (неэтичных) решений, не основанных на тщательном исследовании фактических обстоятельств конкретного дела.

При хранении и использовании данных необходимо обеспечивать: надлежащий уровень защищенности данных; недопустимость несанкционированного доступа к данным; недопустимость неправомерного копирования, распространения и уничтожения информации; своевременное проведение служебного расследования инцидентов, связанных с несанкционированным доступом к данным и иных неправомерных действий. При обращении с информацией сотрудникам правоохранительных органов рекомендовано: «проявлять соразмерность, раз-

<sup>1</sup> См.: Криминалистика будущего. Какая она? // Центр экспертиз при Институте судебных экспертиз и криминалистики МЮ РФ. URL: <https://ceur.ru/news/specproekty/item311872/> (дата обращения: 26.03.2022).

умность, корректность и сдержанность при реализации полномочий по обеспечению безопасности и конфиденциальности информации»<sup>1</sup>, полученной в связи с выполнением служебных обязанностей.

Возникает также вопрос о том, способны ли системы ИИ в настоящее время успешно решать нелинейные задачи и можно ли допустить полностью автоматизированное принятие решения в рамках расследования преступлений? На данный момент на оба вопроса следует однозначно ответить отрицательно. Дело в том, что в настоящее время развитие технологий находится на уровне «слабого» ИИ. Он позволяет лишь «имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека при решении задач компьютерного зрения, обработки естественного языка, распознавания и синтеза речи, поддержки принятия решений и других практически значимых задач обработки данных»<sup>2</sup>. Перспективы создания «сильного» ИИ, «...способного подобно человеку мыслить, взаимодействовать, адаптироваться к изменяющимся условиям и решать другие задачи в области обработки информации, ассоциирующиеся с естественным интеллектом человека...»<sup>3</sup> остаются неопределенными.

Внедрение систем ИИ, безусловно, уже сейчас может облегчить и ускорить процесс принятия важных процессуальных и тактических решений за счёт автоматизации этого процесса. Полученные с их помощью данные можно использовать при решении таких тактических задач расследования как планирование следственных и розыскных действий, так и расследования в целом, а также при выдвижении версий, составлении криминалистической характеристики преступления и в розыске.

Вопрос о возможности замены следователя системами ИИ уже неоднократно обсуждался. Если рассматривать эту проблему с точки зрения этики, то необходимо отметить следующее. Системы ИИ анализируют ситуацию только с учетом ранее введенных в нее данных. Системам ИИ не свойственно внутреннее убеждение, формирующееся под влиянием специфики конкретного дела. Машина в любом случае никогда не сможет мыслить как человек. В связи с этим возникает, например, вопрос о том, каким образом система ИИ сможет достоверно устанавливать мотив преступления, являющийся одним из ключевых аспектов, образующий состав преступления и влияющий на тяжесть приговора. Что касается формирования следователем доказательственной базы по многим категориям преступлений, то, по-прежнему, их основу составляют традиционные для криминалистики следы — материальные (следы рук, ног, следы биологического происхождения и пр.) и идеальные. Работа следователя на месте происшествия по их обнаружению, фиксации и изъятию не может быть выполнена ИИ, который можно рассматривать лишь как вспомогательный инструмент.

<sup>1</sup> Приказ МВД России от 26 июня 2020 г. № 460 «Об утверждении Кодекса этики и служебного поведения сотрудников органов внутренних дел Российской Федерации» (п. 14). URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_385622/](http://www.consultant.ru/document/cons_doc_LAW_385622/) (дата обращения: 21.03.2022).

<sup>2</sup> ГОСТ Р 59276 – 2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» (п. 3.6). URL: <https://docs.cntd.ru/document/1200177291> (дата обращения: 26.03.2022).

<sup>3</sup> ГОСТ Р 59276 – 2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» (п. 3.15). URL: <https://docs.cntd.ru/document/1200177291> (дата обращения: 26.03.2022).



По мнению руководителя НИИ криминалистики СК РФ А.А. Бессонова, ИИ не может заменить субъекта расследования, поскольку «...работа следователя настолько многоаспектна, охватывает самые разнообразные проявления жизни и, более того, постоянно требует творческого подхода и креативного мышления, обусловленных уникальностью каждого преступления»<sup>1</sup>. В процессе расследования важны не только хорошее знание законодательства, сбор данных, тщательная обработка поступающей информации, но и сугубо «человеческие» качества, которые невозможно передать машине, как, например, следственная интуиция, а также знание человеческой психологии. Несмотря на то, что системы ИИ уже сейчас могут определять эмоциональное состояние человека путем анализа невербальных признаков поведения, нельзя им доверять производство вербальных следственных действий. При планировании следственных действий следователь должен заранее продумывать ход их проведения, формулировку вопросов к процессуальному участнику и определять их последовательность, а при опасности возникновения конфликтной ситуации вовремя предпринимать меры на устранение её причин. С целью установления истины и обстоятельств преступления, следователь старается проникнуть в душу человека, что не свойственно ИИ. К тому же интеллектуальные системы не обладают эмпатией. «Согласно положениям отечественной психологии субъект любого вида деятельности, в том числе профессиональной, носитель сознания. Именно благодаря сознанию следователь обладает системой убеждений, совестью, способен действовать с учетом этических норм. Таким образом, в категориях психологии деятельности искусственный интеллект не может быть субъектом никакого вида деятельности, в том числе следственной, но выполнять отдельные функции с большей эффективностью он способен» [3, с. 93].

Таким образом, наделение ИИ правосубъектностью недопустимо. Системы ИИ в будущем смогут взять на себя существенную часть интеллектуальной работы, которыми не располагает человеческий мозг, но говорить о полноценной замене следователя не представляется возможным. Следует согласиться с мнением о том, что «...даже при эффективной работе искусственного интеллекта, вряд ли общество в ближайшее время будет готово осудить преступника не на основе доказательств, а на основе вердикта компьютера, вынесенного на основании сложной математической программы, понять которую присяжные не могут» [4, с. 30–31].

Понятно, что деятельность правоохранительных органов в условиях всеохватывающей цифровизации невозможна без оперативного внедрения новых технологий, обеспечивающих эффективный анализ и оценку данных, сопоставление полученных результатов с помощью современного программного обеспечения. В этой ситуации этика в области цифровых технологий, связанных с получением, обработкой и использованием различных данных требует новой культуры работы с данными. Важно уметь работать в современной информационной сфере, взаимодействовать с IT-специалистами, знать как и где искать криминалистически значимую информацию, особенности ее фиксации, грамотно и этично строить диалог с участниками процесса расследования. По мнению В.С. Овчинского, «... для этичного использования ИИ правоохранительными органами предстоит

<sup>1</sup> Руководитель НИИ криминалистики СК РФ: идеальных преступлений не бывает. URL: <https://tass.ru/interviews/12688681> (дата обращения: 26.03.2022).

создать систему государственного и общественного надзора. Ее задачи — предупредить превышение полномочий сотрудниками полиции и следователями и обеспечить верификацию данных, используемых для обучения алгоритмов ИИ» [5, с. 170].

Российская система правоохранительных органов пока не готова к широкому использованию систем ИИ при расследовании преступлений. У сотрудников наблюдается дефицит необходимых компетенций и навыков использования систем ИИ, отсутствует культура работы с данными. В результате из-за риска допустить непреднамеренное нарушение законодательства и создать этические проблемы сотрудники опасаются принимать решения на основе анализа данных, проведенного с применением систем ИИ. Поэтому необходимо периодически проводить обучение и переподготовку сотрудников с целью изучения возможностей работы системами ИИ, где можно отрабатывать необходимые навыки на реальных примерах и искать нестандартные подходы для решения задач в этой сложной, но интересной сфере.

Обобщая изложенное, можно сделать вывод о том, что этичность систем ИИ вероятна, если: при создании программы не допущены (случайно или осознанно) ошибки; алгоритм программы не способен проявлять предвзятость и дискриминацию; созданная программа обладает свойством прозрачности; исключена опасность выхода системы из-под контроля человека; система хранения и обработки данных надежна и не может привести к изменению сохраняемой информации.

Соблюдение принципов этики со стороны субъекта расследования может зависеть от знания специфики и возможностей технологий ИИ, умения налаживать взаимодействие с IT-специалистами, способности критичности оценивать результаты работы систем ИИ. Субъект расследования должен быть в курсе развития новых технологий и понимать, какие последствия (правовые, этические и т.д.) может вызвать их применение. На конференции по искусственному интеллекту В.В. Путин отметил, что развитие ИИ действительно влечет за собой определенные риски, но именно «...от человека зависит, насколько аккуратно он будет распоряжаться этими возможностями»<sup>1</sup>.

Таким образом, соблюдение этических правил должно служить ориентиром для тех, кто разрабатывает системы ИИ, а также пользуется их достижениями при выполнении своих профессиональных функций. Учет этических аспектов при расследовании преступлений является основой эффективной работы с данными, полученными с помощью систем ИИ, предпосылкой установления истинной картины расследуемого события и достижения целей расследования преступлений.

#### Библиографический список

1. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики М.: Норма, 2001. 240 с.
2. Воробьева И.Б. Применение больших данных (big data) при прогнозировании и расследовании преступлений // Вестник Саратовской государственной юридической академии. 2021. № 3 (140). С. 195–202.

<sup>1</sup> См.: Конференция по искусственному интеллекту // Сайт Президента России. URL: <http://www.kremlin.ru/events/president/news/64545> (дата обращения: 21.03.2022).

3. *Воронова Ю.В.* К вопросу о применении искусственного интеллекта в следственной деятельности (психологический аспект) // Создание и развитие модели органов предварительного расследования в Российской империи: материалы Всероссийской научно-практической конференции (Москва, 24 сентября 2020 года) / под общ. ред. Д.Н. Кожухарика. М.: Московская академия Следственного комитета Российской Федерации, 2020. С. 91–94.

4. *Бабич В.Н., Кириллова Е.А.* Обзор отдельных вопросов в области больших данных и искусственного интеллекта / под ред. В.С. Овчинского. М.: ФКУ «ГИАЦ МВД России», 2019. 148 с.

5. *Овчинский В.С.* Этика цифровых технологий в полиции // Этика и «цифра»: Этические проблемы цифровых технологий. М.: РАНХиГС, 2020. 207 с.

#### References

1. *Belkin R.S.* Criminalistics: Problems of Today. Topical Issues of Russian Criminalistics. M.: publishing house Norma, 2001. 240 p.

2. *Vorobyova I.B.* Using the Big Data for Crime Prediction and Investigation // Herald of the Saratov State Law Academy. 2021. No. 3 (140). P. 195–202.

3. *Voronova Yu.V.* To the Issue of Using Artificial Intellect for Investigative Activities (psychological aspect) // Generating and Developing a Model of Preliminary Investigation Organs in the Russian Empire: Materials of the All-Russia scientific-practical conference (Moscow, September 24, 2020) / Ed. By D.N. Kozhukharik. M.: Moscow Academy of the Investigative Committee of the Russian Federation, 2020. P. 91–94.

4. *Babich V.N., Kirillova E.A.* Review of Individual Issues in the Field of the Big Data and Artificial Intellect. Ed. By V.S. Ovchinsky. M.: MIAC at the MIA of Russia, 2019. 148 p.

5. *Ovchinsky V.S.* Ethics of Digital Technologies on the Force // Ethics and Digital Means: Ethical Problems of Digital Technologies. M.: RANE and PA, 2020. 207 p.