ISSN 2500-4255

УДК 343.9
DOI 10.17150/2500-4255.2018.12(6).767-775

КРИМИНОЛОГИЧЕСКИЕ РИСКИ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

И. Р. Бегишев[1], З. И. Хисамова[2]
[1] Казанский инновационный университет им. В. Г. Тимирясова (ИЭУП), г. Казань, Российская Федерация
[2] Краснодарский университет Министерства внутренних дел Российской Федерации, г. Краснодар, Российская Федерация

Информация о статье

Дата поступления
13 ноября 2018 г.

Дата принятия в печать
15 ноября 2018 г.

Дата онлайн-размещения
24 декабря 2018 г.

Ключевые слова
Искусственный интеллект; интеллектуальные технологии; робот; машинное обучение; криминологический риск; криминологическая характеристика; риски применения искусственного интеллекта; угрозы применения искусственного интеллекта; криминальный потенциал искусственного интеллекта; преступления с применением искусственного интеллекта

Аннотация. В современном цифровом мире тематика искусственного интеллекта и сфера разработки интеллектуальных технологий являются крайне актуальными и важными. За полувековую историю искусственный интеллект успел перерасти из теоретической концепции в интеллектуальную систему, способную самостоятельно принимать решения. В числе ключевых преимуществ внедрения искусственного интеллекта в первую очередь отмечается возможность освобождения человечества от рутинной работы и переход к творческой деятельности, на которую машины не способны. По данным международных консалтинговых агентств, инвестиции компаний в цифровую трансформацию к 2021 г. в глобальном масштабе достигнут 58 трлн дол., а в 2030 г. глобальный ВВП вырастет на 14 %, или на 15,7 трлн дол. США, в связи с активным использованием искусственного интеллекта. Однако его стремительное развитие поставило перед государством и обществом необходимость противостоять новым угрозам, связанным со способностью искусственного интеллекта к саморазвитию, в частности необходимость нормативной регуляции его деятельности и противодействия угрозам, возникающим при его функционировании. В статье приведены результаты подробного изучения мнений ведущих ученых, занимающихся социальными аспектами деятельности искусственного интеллекта. Определено, что вопрос правового регулирования правосубъектности искусственного интеллекта, не говоря уже о совершении им юридически значимых действий, на сегодняшний день остается открытым. В настоящее время началось формирование криминологических основ применения искусственного интеллекта, вызванных появлением новых интеллектуальных технологий, что требует принятия действий и решений по предупреждению возможных негативных проявлений его использования и государственному реагированию на них. В статье на основе анализа истории возникновения и развития искусственного интеллекта изложены его ключевые характеристики, несущие в себе криминологические риски, определены виды криминологических рисков применения искусственного интеллекта, предложена авторская классификация указанных рисков. В частности, выделены прямой и косвенный криминологические риски применения искусственного интеллекта. На основе детального анализа авторами выявлена объективная необходимость создания в стране компетентных органов по выработке государственной политики в сфере нормативного правового регулирования искусственного интеллекта, контроля и надзора за его использованием.

CRIMINOLOGICAL RISKS OF USING ARTIFICIAL INTELLIGENCE

Ildar R. Begishev[1], Zarina I. Khisamova[2]
[1] Kazan Innovative University named after V. G. Timiryasov (IEML), Kazan, the Russian Federation
[2] Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Krasnodar, the Russian Federation

Article info

Received
2018 November 13

Accepted
2018 November 15

Available online
2018 December 24

Abstract. The topics of artificial intelligence (AI) and the development of intelligent technologies are highly relevant and important in the modern digital world. Over its fifty years of history, AI has developed from a theoretical concept to an intelligent system capable of making independent decisions. Key advantages of using AI include, primarily, an opportunity for mankind to get rid of routine work and to engage in creative activities that machines are not capable of. According to international consulting agencies, global business investments in digital transformation will reach 58 trillion USD by 2021, while global GDP will grow by 14 %, or 15.7 trillion USD, in connection with the active use of AI. However, its rapid evolvement poses new threats connected with AI's ability to self-develop that the state and the society have to counteract; specifically, they have

ISSN 2500-4255

Keywords
Artificial intelligence; intelligent technology; robot; machine learning; criminological risks; criminological features; risks of using artificial intelligence; threats of using artificial intelligence; criminal capacity of artificial intelligence; crimes involving artificial intelligence

to introduce normative regulation of AI activities and to address threats arising from its functioning. The authors present a thorough analysis of the opinions of leading researchers in the field of social aspects of AI's functioning. They also state that the regulation of the status of AI as a legal personality, not to mention its ability to commit legally meaningful actions, remains an open question today. At present, the process of creating a criminological basis for applying AI, connected with the development of new intelligent technologies, is underway, it requires actions and decisions aimed at preventing possible negative effects of its use and reacting to them on a state level. The authors' analysis of the history of AI's emergence and development has allowed them to outline its key features that pose criminological risks, to determine criminological risks of using AI and to present their own classification of such risks. In particular, they single out direct and indirect criminological risks of using AI. A detailed analysis has allowed the authors to identify an objective need for establishing special state agencies that will develop state policy in the sphere of normative legal regulation, control and supervision over the use of AI.

Введение

Мир находится на пороге новой цифровой эры. Цифровая экономика становится все более важной частью глобальной экономики, открывая новые возможности для бизнеса и устойчивого развития всего мирового сообщества.

Цифровизация сегодня касается не только технологического сектора и цифровых компаний, но и производственных цепочек в самых разных секторах глобальной экономики [1, с. 3]. По данным International Data Corporation, занимающейся изучением мирового рынка информационных технологий и телекоммуникаций, в 2017 г. расходы компаний на цифровую трансформацию в глобальном масштабе составили 958 млрд дол. [2]. По прогнозам аналитиков, в 2018 г. мировые затраты на технологии и сервисы, обеспечивающие цифровые преобразования бизнес-практик, продуктов и организаций, превысят 1,1 трлн дол., а к 2021 г. инвестиции достигнут 58 трлн дол. [3].

Бóльшая часть указанных инвестиций приходится на производственный сектор экономики, преимущественно на внедрение в автоматизированные системы управления технологическими процессами искусственного интеллекта (ИИ). Согласно результатам исследования авторитетной международной компании PwC, специализирующейся в области консалтинга и аудита, в 2030 г. глобальный ВВП вырастет на 14 %, или на 15,7 трлн дол. США, в связи с активным использованием ИИ. Также, по данным компании PwC, 72 % крупнейших корпораций мира считают ИИ фундаментом будущего[1].

ИИ окружает нас повсюду. Мы живем в эпоху больших данных, когда ежедневно обрабатывается огромный объем информации, слишком громоздкой для обработки человеком. Среднестатистический житель планеты использует ИИ намного чаще, чем думает: только 33 % респондентов считают, что они применяют технологию с поддержкой ИИ, в то время как 77 % фактически используют услугу или устройство с ИИ[2].

Стоит отметить, что несомненные плюсы внедрения ИИ, предполагающего освобождение человечества от рутинной работы и переход к творческой деятельности, на которую машины не способны, видят не только крупные корпорации, но и обычные жители: 61 % из опрошенных 6 тыс. чел. заявили, что, по их мнению, ИИ сделает мир лучше[3].

Так ли это на самом деле? Знаем ли мы, современное общество, что такое ИИ и какие риски несет в себе его создание и оборот? Сможем ли извлечь преимущества из применения ИИ, избежав негативных последствий? Существуют ли регулятивные механизмы контроля ИИ? Готово ли отечественное законодательство к регулированию ситуаций, когда ИИ станет участником посягательств на охраняемые законом правоотношения? И не станет ли заглавие книги Д. Баррата «Последнее изобретение человечества: Искусственный интеллект и конец эры Homo sapiens» [4] пророческим?

В рамках настоящего исследования предпринята попытка найти ответы на столь неоднозначные и одновременно животрепещущие вопросы, в связи с чем была проанализирована история возникновения и развития ИИ [5–7].

[1] Искусственный интеллект: не упустить выгоду // PwC. URL: https://www.pwc.ru/ru/press-releases/2017/artificial-intelligence-enlargement.html.

[2] What Consumers Really Think About AI // Pega. URL: https://www1.pega.com/system/files/resources/2017-11/what-consumers-really-think-of-ai-infographic.pdf.

[3] Global Artificial Intelligence Survey // Arm Limited. URL: https://www.arm.com/solutions/artificial-intelligence/survey.

История возникновения и развития ИИ

Человечество с древнейших времен не покидала мысль о создании устройств или приспособлений, способных упростить жизнь. Механизировав и автоматизировав тяжелый физический труд, общество задумалось о создании машины, способной выполнять интеллектуальную (умственную) работу — сугубо человеческую прерогативу. К 1950-м гг. в научном сообществе появилось поколение молодых ученых, математиков и философов, с концепцией ИИ, культурно ассимилированного в их умах. Одним из таких людей был А. Тьюринг, который сегодня считается основоположником теории ИИ. Он выдвинул тезис о том, что машины, как и люди, способны использовать доступную информацию, а также разум, чтобы решать проблемы и принимать решения [8]. Кроме того, им был описан тест (впоследствии получивший имя автора), позволяющий определить, когда машины смогут сравняться с человеком [9]. Однако идеи Тьюринга в середине XX в. не могли быть воплощены в жизнь в силу ряда объективных причин. До 1949 г. компьютеры не имели ключевой характеристики для интеллекта — они могли только выполнять команды, а не запоминать их. Вычислительная техника была чрезвычайно дорогой: например, стоимость аренды компьютера доходила до 200 тыс. дол. в месяц [там же]. Только престижные университеты и крупные технологические компании могли себе их позволить. И, наконец, исследования возможностей развития ИИ [10] требовали финансирования и государственной поддержки, что также было весьма непростой задачей.

Шесть лет спустя доказательство возможности создания ИИ было представлено на конференции, организованной Д. Маккарти и М. Мински в Дартмутском университете. А. Ньюэллом, К. Шоу и Г. Саймоном была продемонстрирована программа «Теоретика логики» (The Logic Theorist), предназначенная для имитации навыков решения проблем человека. Большинство исследователей склонны считать указанную программу первым прототипом ИИ. Стоит отметить, что Д. Маккарти на упомянутом мероприятии было придумано само понятие ИИ (англ. artificial intelligence, AI). Конференция в Дартмуте стала отправной точкой исследований ИИ [11], которые на протяжении 70 лет переживали то бурный всплеск, то крайнее затишье.

Период с 1957 по 1974 г. стал эпохой расцвета изучения ИИ: увеличилась производительность, доступность и объем памяти компьютеров, значительный прогресс наблюдался в развитии алгоритмов машинного обучения. Первые прототипы ИИ в начале 60-х гг., такие как компьютерная программа General Problem Solver, разработанная А. Ньюэллом и Г. Саймоном, и Eliza Д. Вайзенбаума, имели многообещающее будущее в решении ряда проблем, особенно в части интерпретации разговорного языка. В 1971 г. корпорация Intel выпустила свой первый коммерчески доступный микропроцессор [3, p. 8]. Эти успехи, а также пропаганда ведущих исследователей убедили государственные учреждения, такие как Агентство передовых оборонных исследовательских проектов США, финансировать исследования ИИ в нескольких учреждениях. Правительство было весьма заинтересовано в механизме, который мог бы транскрибировать и переводить устную речь, а также обладал бы высокой производительностью в обработке данных. Оптимизм был высок, а ожидания еще выше: в 1970 г. М. Мински утверждал, что в течение трех — восьми лет будет создана машина с интеллектом среднего человека [9].

Однако в конце 70-х гг. научное сообщество столкнулось с неожиданной проблемой недостатка вычислительных мощностей: компьютеры просто не могли хранить достаточно информации или обрабатывать ее достаточно быстро. Вплоть до середины 80-х гг. исследования ИИ замедлились и не имели значимых результатов, пока Д. Хопфилдом и Д. Румельхартом не были популяризированы методы глубокого обучения, ставшие возможными благодаря расширению алгоритмического инструментария и увеличению средств машинного обучения. Одновременно с ними Э. Фейгенбаум представил экспертные системы, которые имитировали процесс принятия решений экспертом-человеком. В указанный период интерес к изучению и развитию ИИ был проявлен и японским правительством: в 1982–1990 гг. оно инвестировало 400 млн дол. в проект создания «компьютера пятого поколения» с целью революционизации компьютерной обработки, внедрения логического программирования и улучшения ИИ [12].

Несмотря на то что большинство амбициозных целей создания «компьютера пятого поколения» не было достигнуто, все же можно утверждать, что проект стал новым толчком развития ИИ, продолжающимся по сей день.

Так, в 1997 г. действующий чемпион мира по шахматам гроссмейстер Г. К. Каспаров был побежден компьютерной программой компании

IBM Deep Blue. Этот широко разрекламированный матч стал первым проигрышем компьютеру действующего чемпиона мира по шахматам [13]. В том же году на операционной системе Windows была реализована программа распознавания речи, разработанная компанией Dragon Systems. Это стало еще одним большим шагом вперед, но в направлении устного перевода. Казалось, что не было проблем, с которыми машины не могли справиться. Даже человеческие эмоции стали доступны для машины, о чем свидетельствует Kismet — робот, который мог распознавать и отображать эмоции и мимику. Начало 2000-х гг. ознаменовалось победой автомобиля-робота команды Стэндфордского университета в DARPA Grand Challenge — соревнованиях автомобилей-роботов, созданием нейронных сетей, появлением первого виртуального ассистента Siri и победой программы Alpha Go с глубоким самообучением компании Google в матче с Ли Седолем, чемпионом мира по игре Go [3, p. 8].

На сегодняшний день наблюдается активное прикладное применение ИИ во всех предметных областях и непрекращающееся расширение его возможностей. Выделяют несколько ключевых областей развития ИИ:

– крупномасштабное машинное обучение — разработка алгоритмов обучения, а также масштабирование существующих алгоритмов для работы с очень большими наборами данных;

– глубокое обучение — модель, составленная из входных «сигналов», таких как изображение или аудио, и нескольких спрятанных слоев подмодели, которые служат входными данными для следующего слоя и в конечном счете выходными данными или функцией активации;

– обработка естественного языка — алгоритмы, которые обрабатывают ввод на человеческом языке и преобразуют его в понятные представления;

– совместные системы — модели и алгоритмы, помогающие разрабатывать автономные системы, которые могут работать совместно с другими системами и людьми;

– «компьютерное зрение» (анализ изображений) — процесс вытягивания релевантной информации от изображения или наборов изображений для предварительных классификации и анализа;

– алгоритмическая теория игр и вычислительный социальный выбор — системы, которые учитывают экономические и социальные аспекты ИИ;

– робототехника в приложениях (роботизированная автоматизация процессов) — автоматизация повторяющихся задач и общих процессов, таких как ИТ, обслуживание клиентов и продаж[4].

В рамках настоящего исследования мы исходили из понимания ИИ как собирательного термина интеллектуальной компьютерной программы (системы ИИ, ИИ-технологий), которая может анализировать окружающую среду, думать, учиться и реагировать в ответ на то, что она «чувствует». В широком смысле слова ИИ — некая интеллектуальная система, способная самостоятельно принимать решения.

Данная система представляет собой направление разработки компьютерных функций, связанных с человеческим интеллектом, таких как рассуждение, обучение и решение проблем. Иными словами, ИИ — это перенос человеческих возможностей мыследеятельности в плоскость компьютерных и информационных технологий, но уже без свойственных человеку пороков [14, с. 9]. Ученые, занимающиеся данным вопросом, усиленно изучают перспективы признания электронного лица и место человека в таком мире [15].

Мы солидарны с мнением И. В. Понкина и А. И. Редькиной в том, что ИИ — это искусственная сложная кибернетическая компьютерно-программно-аппаратная система (электронная, в том числе виртуальная, электронно-механическая, био-электронно-механическая или гибридная) с когнитивно-функциональной архитектурой и собственными или релевантно доступными (приданными) вычислительными мощностями необходимых емкостей и быстродействия [16, с. 95].

К сходным выводам пришел П. М. Морхат, считающий, что ИИ — это полностью или частично автономная самоорганизующая (самоорганизующаяся) компьютерно-аппаратно-программная виртуальная (virtual) или киберфизическая (cyber-physical), в том числе биокибернетическая (bio-cybernetic), система (юнит), наделенная/обладающая способностями и возможностями [17, с. 69]. При этом автор отмечает, что активное использование юнитов ИИ уже сегодня влечет возникновение в правовом пространстве множественных неопределенностей, сложностей, проблем [там же, с. 70]. Мы разделяем данную позицию.

В современной научной и технической литературе приводится достаточно много различных

[4] Artificial intelligence and life in 2030 // Stanford University. 2016. P. 9. URL: https://ai100.stanford.edu/sites/default/files/ai_100_report_0831fnl.pdf.

классификаций систем ИИ и возможностей их применения [18–20]. Однако, принимая во внимание методологию настоящего исследования, мы придерживались классификации ИИ, учитывающей прикладные аспекты современных информационно-телекоммуникационных технологий.

Стоит отметить, что в исследовании компании PwC все виды ИИ разделены на две группы в зависимости от взаимодействия с человеком. Так, к видам ИИ, взаимодействующего с людьми, относят специальные устойчивые системы, такие как вспомогательный интеллект, помогающий людям выполнять задачи быстрее и лучше. Устойчивые системы неспособны обучаться в их взаимодействиях. К указанной группе также принято относить адаптивный (дополненный) интеллект, который помогает людям принимать правильные решения и способен к самообучению во время взаимодействия с человеком.

Во вторую группу видов ИИ, не взаимодействующего с человеком, включают автоматизированный интеллект, предназначенный для автоматизации механических/когнитивных и рутинных задач. Его функционирование не связано с выполнением новых задач и находится в сфере автоматизации существующих задач. К указанной группе также относится автономный интеллект, который по своему функционалу и возможностям превосходит все предыдущие и может представлять угрозу для человечества и общества. Такой ИИ способен адаптироваться к различным ситуациям и действовать самостоятельно без участия человека[5], совершая, например, кражу личности [21].

Ключевые характеристики ИИ, несущие в себе криминологические риски

Тему угрозы ИИ для человечества впервые поднял профессор Оксфордского университета Н. Бостром в своей книге Superintelligence: Paths, Dangers, Strategies, которая стала бестселлером по версии американской ежедневной газеты The New York Times и является одной из книг, обязательных для прочтения по рекомендациям Б. Гейтса и И. Маска[6]. В ней профессор Бостром утверждает, что основная угроза для человечества не изменение климата, не пандемия и не ядерная зима; это неизбежное создание общего машинного интеллекта, большего, чем наш собственный [22]. Аналогичный тезис был высказан и величайшим ученым-космологом С. Хокингом в его последней книге: появление сверхумных машин станет либо лучшим, либо худшим событием в истории человечества. Умные компьютеры будут наделены собственной волей, которая совсем не обязательно совпадет с нашей. Человек эволюционирует с естественной скоростью, поэтому не сможет тягаться с искусственным разумом. Эту гонку вооружений мы можем и не выиграть, так что единственно верное решение — ее предотвратить [23].

По прогнозам Н. Бострома, через 60 лет ИИ станет серьезной угрозой человечеству. К 2022 г. сходство процессов мышления робота и человека будет равняться примерно 10 %, к 2040 г. — 50 %, а в 2075 г., согласно закону Мура, мыслительные процессы роботов уже нельзя будет отличить от человеческих, они достигнут 95 % [22].

На наш взгляд, А. Э. Радутный весьма удачно резюмировал опасения ученых:

– благодаря способности к саморазвитию ИИ может стать искусственным суперинтеллектом (ИСИ) [24];

– у ИСИ будут свои потребности и цели (он может быть менее гуманным, чем разумный инопланетянин);

– ИСИ может попытаться использовать людей против их воли (например, получить доступ к ресурсам);

– ИСИ, возможно, пожелает быть единственным видом на Земле;

– люди как система удобно сгруппированных атомов могут представлять интерес для ИСИ в качестве ресурса;

– человечество не готово к встрече с ИСИ и не будет готово еще много лет;

– человечество должно научиться держать ИИ под достаточным контролем [25].

Необходимо отметить, что не только величайшие умы человечества обеспокоены угрозами, которые несет развитие ИИ. Согласно независимому глобальному опросу, проведенному инновационными компаниями Northstar и ARM, чуть более трети опрошенных думают, что ИИ уже оказывает заметное влияние на их повседневную жизнь[7]. Несмотря на то что более половины жителей ожидают лучшее будущее для общества благодаря ИИ, пятая часть опрошенных ожидает худшего. Существуют и региональ-

[5] Искусственный интеллект: не упустить выгоду.

[6] Best Selling Science Books // The New York Times. 2014. Sept. 8.

[7] В рамках онлайн-опроса было изучено мнение 3 млн 938 тыс. чел. во всем мире (преимущественно в странах Северной Америки, Западной Европы и Юго-Восточной Азии).

ные различия. Жители североамериканского континента и европейцы выразили обеспокоенность относительно надежности машин с ИИ, в то время как в странах Азии существует подлинное опасение, что машины с ИИ становятся более умными, чем люди[8]. В целом подавляющее большинство опрошенных (85 %) обеспокоены обеспечением безопасности технологии ИИ.

Рассмотрим данную проблему с учетом различных практик применения ИИ.

Так, проблема обеспечения безопасности конфиденциальной информации, в том числе проблема обеспечения кибербезопасности с использованием ИИ, является одной из ключевых для всех субъектов цифровой экономики [26].

Согласно данным аналитического центра компании InfoWatch — крупнейшего российского производителя решений для защиты организаций от внутренних и внешних угроз, а также от информационных атак, в первом полугодии 2017 г. было зарегистрировано более 920 инцидентов, связанных с утечкой конфиденциальной информации из организаций различных форм собственности. Данные об инцидентах включают все утечки во всех зарубежных странах, сведения о которых опубликованы в средствах массовой информации, блогосфере, социальных сетях и на иных сетевых ресурсах [27, с. 28].

Для решения указанной проблемы компании проводят постоянные исследования в рассматриваемой сфере. К примеру, американская корпорация Google разработала программу под названием Federated Learning, в которой облегченная версия программного обеспечения Sensorflow позволяет использовать ИИ на смартфоне и обучать его. Вместо сбора и хранения информации в одном месте, на серверах Google, для последующей работы с новыми алгоритмами процесс обучения происходит непосредственно на мобильном устройстве каждого пользователя. По сути, процессор телефона используется как вспомогательное средство обучения ИИ. Преимущество этого приложения заключается в том, что конфиденциальная информация никогда не покидает устройство пользователя, а обновления приложений применяются в режиме реального времени. Позже информация собирается Google анонимно и используется для внесения общих уточнений в приложение [28].

Таким образом, можно предположить, что ИИ может совершить общественно опасное деяние, связанное с нарушением конфиденциальности охраняемой законом информации.

Вопросами использования ИИ в преступных целях обеспокоено мировое сообщество. Так, в начале 2017 г. ФБР провело крупную конференцию, посвященную вопросам использования ИИ правоохранительными органами и криминалом. На конференции было отмечено: данные Интерпола, Европола, ФБР и правоохранительных органов других стран, результаты исследований ведущих университетов указывают на отсутствие активности криминальных структур по созданию своих разработок в сфере ИИ [29, с. 149]. По мнению В. С. Овчинского, несмотря на отсутствие сведений о разработках кибепреступников в сфере ИИ, потенциальная возможность такого явления существует: «У киберкриминала есть из чего выбрать для создания собственных мощных платформ ИИ. Практически все разработки ИИ с открытым исходным кодом представляют собой контейнеры. Контейнер — это платформа, на которой при помощи API могут монтироваться любые сторонние программы, сервисы, базы данных и т. п. Если раньше каждый при создании собственной программы или сервиса должен был от начала до конца первоначально разработать алгоритмы, а затем, пользуясь тем или иным языком программирования, перевести их в код, то сегодня возможно создавать продукты и сервисы так же, как строители строят дом — из стандартных, доставленных на стройплощадку деталей» [там же, с. 150].

Таким образом, процессы применения ИИ в преступных целях имеют повышенную общественную опасность [30]. Однако использование коммуникаций с открытым исходным кодом для оценки преступности видится перспективной идеей [31], в том числе в эпоху больших данных [32].

Согласно исследованиям, основными наиболее активными сферами внедрения ИИ являются медицинские приложения (программы диагностики заболеваний), цифровые сервисы — помощники, автономные транспортные средства[9]. При этом, например, ошибка ИИ программы диагностики заболеваний [33], поставившей неверный диагноз, может повлечь неправильное лечение больного и, как следствие, возможное нарушение его здоровья.

[8] AI today. AI tomorrow. Awareness, acceptance and anticipation of AI: a global consumer perspective. URL: https://pages.arm.com/rs/312-SAX-488/images/arm-ai-survey-report.pdf.

[9] AI today. AI tomorrow. Awareness, acceptance and anticipation of AI: a global consumer perspective.

Отметим, что изучение юридических аспектов, связанных с общественно опасными последствиями применения ИИ, представляет собой самостоятельный пласт серьезных и достаточно глубоких уголовно-правовых исследований, результатом которых должно стать формирование концептуально новой правовой модели регулирования отношений в указанной сфере. Вместе с тем в рамках настоящего исследования авторами выделены ключевые риски (потенциальные угрозы) применения ИИ, что, в свою очередь, должно не только послужить основой для дальнейших глубоких теоретических изысканий в криминологии, но и в целом стать импульсом для проведения исследований в рамках иных наук криминального цикла.

Проведенный анализ тенденций в области создания и использования ИИ позволил нам выделить два вида криминологических рисков применения ИИ — прямой и косвенный.

Прямой криминологический риск применения ИИ — риск, связанный с непосредственным действием на человека и гражданина той или иной опасности, вызванной применением ИИ. К таким рискам можно отнести:

– умышленное совершение системой ИИ общественно опасного посягательства на жизнь и здоровье человека; свободу, честь и достоинство личности; конституционные права и свободы человека и гражданина; общественную безопасность; мир и безопасность человечества, повлекшего общественно опасные последствия;

– умышленные действия с программным обеспечением системы ИИ, повлекшие общественно опасные последствия.

Косвенный криминологический риск применения ИИ — риск, связанный с непреднамеренными опасностями в контексте применения ИИ. К таким рискам можно отнести:

– случайные ошибки в программном обеспечении системы ИИ (ошибки, допущенные разработчиком системы ИИ);

– ошибки, совершенные системой ИИ в процессе его работы (ошибки, допущенные системой ИИ).

Выводы

Изложенная в работе информация подтверждает существование высоких криминологических рисков применения ИИ, заключенных как в самой интеллектуальной технологии, так и в слабой теоретической подготовленности криминологии к изучению рассматриваемой проблемы.

В связи с этим первоочередными видятся мероприятия по созданию федерального органа исполнительной власти Российской Федерации, осуществляющего функции по выработке государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере применения ИИ, подготовке законодательства в области создания и использования ИИ, разработке юридических моделей предупреждения криминального поведения ИИ, в частности определению криминологических рисков его применения.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Хисамова З. И. Международный опыт уголовно-правового противодействия преступлениям в сфере цифровой экономики / З. И. Хисамова. — Краснодар : Изд-во Краснодар. ун-та МВД России, 2018. — 119 с.

2. Rutten P. Worldwide AI Server Infrastructure Forecast, 2018–2022 [Electronic resource] / P. Rutten // Analyze the future. — 2018. — Mode of access: https://www.idc.com/getdoc.jsp?containerId=US44002018.

3. McWaters R. J. The New Physics of Financial Services. Part of the Future of Financial Services series. Understanding how artificial intelligence is transforming the financial ecosystem [Electronic resource] / R. J. McWaters // Deloitte, World Economic Forum. 2018. — 167 p. — Mode of access: http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf.

4. Баррат Д. Последнее изобретение человечества: Искусственный интеллект и конец эры Homo sapiens : пер. с англ. / Д. Баррат. — М. : Альпина нон-фикшн, 2015. — 304 с.

5. Spector L. Evolution of artificial intelligence / L. Spector // Artificial Intelligence. — 2006. — Vol. 170, iss. 18. — P. 1251–1253.

6. Goertzel B. Human-level artificial general intelligence and the possibility of a technological singularity: A reaction to Ray Kurzweil's The Singularity Is Near, and McDermott's critique of Kurzwei / B. Goertzel // Artificial Intelligence. — 2007. — Vol. 171, iss. 18. — P. 1161–1173.

7. Boyd R. Technology, innovation, employment and power: Does robotics and artificial intelligence really mean social transformation? / R. Boyd, R. J. Holton // Journal of Sociology. — 2017. — Vol. 54, iss. 3. — P. 331–345.

8. Turing A. Computing Machinery and Intelligence / A. Turing // Mind, New Series. — 1950. — Vol. 59, № 236. — P. 433–460.

9. Rockwell A. The History of Artificial Intelligence [Electronic resource] / A. Rockwell // Harvard University. — Mode of access: http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence.

10. Wirth N. Hello marketing, what can artificial intelligence help you with? / N. Wirth // International Journal of Market Research. — 2017. — Vol. 60, iss. 5. — P. 435–438.

11. Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. August 31, 1955 / J. McCarthy [et al.] // AI Magazine. — 2006. — Vol. 27, № 4. — P. 12–14. — DOI: https://doi.org/10.1609/aimag.v27i4.1904.

12. Растригин Л. А. С компьютером наедине / Л. А. Растригин. — М. : Радио и связь, 1990. — 224 с.

13. Campbell M. Deep Blue / M. Campbell, A. J. Hoane Jr., Hsu Feng-hsiung // Artificial Intelligence. — 2002. — Vol. 134, iss. 1–2. — P. 57–83.

14. Афанасьев А. Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? / А. Ю. Афанасьев // Библиотека криминалиста. Научный журнал. — 2018. — № 3 (38). — С. 28–34.

15. Carriço G. The EU and artificial intelligence: A human-centred perspective / G. Carriço // European View. — 2018. — Vol. 17, iss. 1. — P. 29–36.

16. Понкин И. В. Искусственный интеллект с точки зрения права / И. В. Понкин, А. И. Редькина // Вестник РУДН. Сер.: Юридические науки. — 2018. — Т. 22, № 1. — С. 91–109.

17. Мохат П. М. Искусственный интеллект: правовой взгляд / П. М. Мохат. — М. : Буки Веди, 2017. — 257 с.

18. Amores J. Multiple instance classification: Review, taxonomy and comparative study / J. Amores // Artificial Intelligence. — 2013. — Vol. 201. — P. 81–105.

19. Núñez-Tabales J. M. Commercial properties prices appraisal: Alternative approach based on neural networks / J. M. Núñez-Tabales, J. Rey-Carmona Francisco, J. M. Caridad y Ocerinm // International Journal of Artificial Intelligence. — 2016. — Vol. 14, № 1. — P. 53–70.

20. Specialization: A new way to improve intelligent systems / J. A. Román [et al.] // International Journal of Artificial Intelligence. — 2015. — Vol. 13, № 1. — P. 58–73.

21. Marron D. Alter Reality: Governing the Risk of Identity Theft / D. Marron // The British Journal of Criminology. — 2008. — Vol. 48, iss. 1. — P. 20–38.

22. Bostrom N. Superintelligence: Paths, Dangers, Strategies / N. Bostrom. — Oxford : Oxford Univ. Press, 2014. — 390 p.

23. Hawking S. Brief Answers to the Big Questions / S. Hawking. — London : Random House LLC, 2018. — 256 p.

24. Rajan K. Towards a science of integrated AI and Robotics / K. Rajan, A. Saffiotti // Artificial Intelligence. — 2017. — Vol. 247. — P. 1–9. — DOI: 10.1016/j.artint.2017.03.003.

25. Radutniy O. E. Criminal liability of the artificial intelligence / O. E. Radutniy // Problems of legality. — 2017. — № 138. — P. 132–141.

26. Wilner A. S. Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation / A. S. Wilner // International Journal. — 2018. — Vol. 73, iss. 2. — P. 308–316.

27. Бегишев И. Р. Синдром безопасной атаки: юридико-психологический феномен / И. Р. Бегишев // Юридическая психология. — 2018. — № 2. — С. 27–30.

28. Vincent J. Google is testing a new way of training its AI algorithms directly on your phone [Electronic resource] / J. Vincent // The Verge. — 2017. — Mode of access: https://www.theverge.com/2017/4/10/15241492/google-ai-user-data-federated-learning.

29. Овчинский В. С. Криминология цифрового мира : учебник / В. С. Овчинский. — М. : Норма, 2018. — 352 с.

30. Wagen W. van der. From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks / W. van der Wagen, W. Pieters // The British Journal of Criminology. — 2015. — Vol. 55, iss. 3. — P. 578–595. — DOI: https://doi.org/10.1093/bjc/azv009.

31. Williams M. L. Crime Sensing with Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns / M. L. Williams, P. Burnap, L. Sloan // The British Journal of Criminology. — 2017. — Vol. 57, iss. 2. — P. 320–340. — DOI: https://doi.org/10.1093/bjc/azw031.

32. Smith G. J. D. The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach / G. J. D. Smith, L. B. Moses, J. Chan // The British Journal of Criminology. — 2017. — Vol. 57, iss. 2. — P. 259–274. — DOI: https://doi.org/10.1093/bjc/azw096.

33. Momi E. De. Robotic and artificial intelligence for keyhole neurosurgery: The RO-BOCAST project, a multi-modal autonomous path planner / E. De. Momi, G. Ferrigno // Proceedings of the Institution of Mechanical Engineers, Part H: Journal of Engineering in Medicine. — 2010. — Vol. 224, iss. 5. — P. 715–727. — DOI: 10.1243/09544119JEIM585.

REFERENCES

1. Khisamova Z. I. *Mezhdunarodnyi opyt ugolovno-pravovogo protivodeistviya prestupleniyam v sfere tsifrovoi ekonomiki* [International experience of criminal law counteraction to crimes in the sphere of digital economy]. Krasnodar University of the Ministry of Internal Affairs of the Russian Federation Publ., 2018. 119 p.

2. Rutten P. Worldwide AI Server Infrastructure Forecast, 2018–2022. *Analyze the future*, 2018. Available at: https://www.idc.com/getdoc.jsp?containerId=US44002018.

3. McWaters R. J. The New Physics of Financial Services. Part of the Future of Financial Services series. Understanding how artificial intelligence is transforming the financial ecosystem. *Deloitte, World Economic Forum. 2018*. 167 p. Available at: http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf.

4. Barrat J. *Our Final Invention. Artificial Intelligence and the End of the Human Era*. New York, St. Martin`s Press, 2013. (Russ. ed.: Barrat J. *Poslednee izobretenie chelovechestva: Iskusstvennyi intellekt i konets ery Homo sapiens.* Moscow, Al'pina Non-Fikshn Publ., 2015. 304 p.).

5. Spector L. Evolution of artificial intelligence. *Artificial Intelligence*, 2006, vol. 170, iss. 18, pp. 1251–1253.

6. Goertzel B. Human-level artificial general intelligence and the possibility of a technological singularity: A reaction to Ray Kurzweil's The Singularity Is Near, and McDermott's critique of Kurzwei. *Artificial Intelligence*, 2007, vol. 171, iss. 18, pp. 1161–1173.

7. Boyd R., Holton R. J. Technology, innovation, employment and power: Does robotics and artificial intelligence really mean social transformation? *Journal of Sociology*, 2017, vol. 54, iss. 3, pp. 331–345.

8. Turing A. Computing Machinery and Intelligence. *Mind, New Series,* 1950, vol. 59, no. 236, pp. 433–460.

9. Rockwell A. The History of Artificial Intelligence. *Harvard University*. Available at: http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence.

10. Wirth N. Hello marketing, what can artificial intelligence help you with? *International Journal of Market Research*, 2017, vol. 60, iss. 5, pp. 435–438.

11. McCarthy J., Minsky M. L., Rochester N., Shannon C. E. Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. August 31, 1955. *AI Magazine,* 2006, vol. 27, no. 4, pp. 12–14. DOI: https://doi.org/10.1609/aimag.v27i4.1904.

12. Rastrigin L. A. *S komp'yuterom naedine* [One on one with the computer]. Moscow, Radio i Svyaz' Publ., 1990. 224 p.

13. Campbell M., Hoane A. J. Jr., Feng-hsiung Hsu. Deep Blue. *Artificial Intelligence*, 2002, vol. 134, iss. 1–2, pp. 57–83.

14. Afanasyev A. Yu. Artificial intelligence or intellect of the subjects of detection, disclosure and investigation of crimes: what will win? *Biblioteka kriminalista = Library of a Criminalist*, 2018, no. 3 (38), pp. 28–34. (In Russian).

15. Carriço G. The EU and artificial intelligence: A human-centred perspective. *European View*, 2018, vol. 17, iss. 1, pp. 29–36.

16. Ponkin I. V., Redkina A. I. Artificial Intelligence from the Point of View of Law. *Vestnik RUDN. Seriya: Yuridicheskie nauki = RUDN Journal of Law,* 2018, vol. 22, no. 1, pp. 91–109. (In Russian).

17. Morkhat P. M. *Iskusstvennyi intellekt: pravovoi vzglyad* [Artificial Intelligence: a Legal Outlook]. Moscow, Buki Vedi Publ., 2017. 257 p.

18. Amores J. Multiple instance classification: Review, taxonomy and comparative study. *Artificial Intelligence*, 2013, vol. 201, pp. 81–105.

19. Núñez-Tabales J. M., Rey-Carmona Francisco J., Caridad y Ocerinm J. M. Commercial properties prices appraisal: Alternative approach based on neural networks. *International Journal of Artificial Intelligence*, 2016, vol. 14, no. 1, pp. 53–70.

20. Román J. A., Rodríguez S., Corchado J. M., Carrascosa C., Ossowski S. Specialization: A new way to improve intelligent systems. *International Journal of Artificial Intelligence*, 2015, vol. 13, no. 1, pp. 58–73.

21. Marron D. Alter Reality: Governing the Risk of Identity Theft. *The British Journal of Criminology*, 2008, vol. 48, iss. 1, pp. 20–38.

22. Bostrom N. *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press, 2014. 390 p.

23. Hawking S. *Brief Answers to the Big Questions*. London, Random House LLC, 2018. 256 p.

24. Rajan K., Saffiotti A. Towards a science of integrated AI and Robotics. *Artificial Intelligence*, 2017, vol. 247, pp. 1–9. DOI: 10.1016/j.artint.2017.03.003.

25. Radutniy O. E. Criminal liability of the artificial intelligence. *Problems of Legality*, 2017, no. 138, pp. 132–141.

26. Wilner A. S. Cybersecurity and its discontents: Artificial Intelligence, the Internet of Things, and digital misinformation. *International Journal,* 2018, vol. 73, iss. 2, pp. 308–316.

27. Begishev I. R. The Secure Attack Syndrome: A Legal and Psychological Phenomenon. *Yuridicheskaya psikhologiya = Legal Psychology,* 2018, no. 2, pp. 27–30. (In Russian).

28. Vincent J. Google is testing a new way of training its AI algorithms directly on your phone. *The Verge*, 2017. Available at: https://www.theverge.com/2017/4/10/15241492/google-ai-user-data-federated-learning.

29. Ovchinskii V. S. *Kriminologiya tsifrovogo mira* [Criminology of the Digital World]. Moscow, Norma Publ., 2018. 352 p.

30. Wagen W. van der, Pieters W. From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *The British Journal of Criminology*, 2015, vol. 55, iss. 3, pp. 578–595. DOI: https://doi.org/10.1093/bjc/azv009.

31. Williams M. L., Burnap P., Sloan L. Crime Sensing with Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns. *The British Journal of Criminology,* 2017, vol. 57, iss. 2, pp. 320–340. DOI: https://doi.org/10.1093/bjc/azw031.

32. Smith G. J. D., Moses L. B., Chan J. The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach. *The British Journal of Criminology*, 2017, vol. 57, iss. 2, pp. 259–274. DOI: https://doi.org/10.1093/bjc/azw096.

33. Momi E. De., Ferrigno G. Robotic and artificial intelligence for keyhole neurosurgery: The RO-BOCAST project, a multi-modal autonomous path planner. *Proceedings of the Institution of Mechanical Engineers, Part H: Journal of Engineering in Medicine,* 2010, vol. 224, iss. 5, pp. 715–727. DOI: 10.1243/09544119JEIM585.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Бегишев Ильдар Рустамович — старший научный сотрудник Казанского инновационного университета им. В. Г. Тимирясова (ИЭУП), кандидат юридических наук, заслуженный юрист Республики Татарстан, г. Казань, Российская Федерация; e-mail: begishev@mail.ru.

Хисамова Зарина Илдузовна — начальник отделения планирования и координации научной деятельности научно-исследовательского отдела Краснодарского университета Министерства внутренних дел Российской Федерации, кандидат юридических наук, г. Краснодар, Российская Федерация; e-mail: alise89@inbox.ru.

ДЛЯ ЦИТИРОВАНИЯ

Бегишев И. Р. Криминологические риски применения искусственного интеллекта / И. Р. Бегишев, З. И. Хисамова // Всероссийский криминологический журнал. — 2018. — Т. 12, № 6. — С. 767–775. — DOI: 10.17150/2500-4255.2018.12(6).767-775.

INFORMATION ABOUT THE AUTHORS

Begishev, Ildar R. — Head, Senior Researcher, Kazan Innovative University named after V. G. Timiryasov (IEML), Ph. D. in Law, Honored Lawyer of the Republic of Tatarstan, Kazan, the Russian Federation; e-mail: begishev@mail.ru.

Khisamova, Zarina I. — Head, Department of Planning and Coordination of Research Activities, Research Department, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation, Ph. D. in Law, Krasnodar, the Russian Federation; e-mail: alise89@inbox.ru.

FOR CITATION

Begishev I. R., Khisamova Z. I. Criminological risks of using artificial intelligence. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2018, vol. 12, no. 6, pp. 767–775. DOI: 10.17150/2500-4255.2018.12(6).767-775. (In Russian).