Научная статья

УДК 343.34:004.8

<https://doi.org/10.24866/1813-3274/2021-3/153-165>

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРЕСТУПНЫХ ЦЕЛЯХ: УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА*

Р. И. Дремлюга¹, Дальневосточный федеральный университет,
г. Владивосток, Россия
E-mail: dreamluck@yandex.ru

Аннотация. Искусственный интеллект активно используется во многих сферах человеческой жизни. Использование систем искусственного интеллекта повышает эффективность деятельности, снижает издержки и увеличивает производительность. Предполагается, что такое продуктивное средство в скором времени будет активно использоваться в преступных целях. В статье проводится анализ понятия «искусственный интеллект» и его отличительных характеристик. Автор приходит к выводу, что современные системы искусственного интеллекта обучаются, а не программируются, что снижает целесообразность возложения ответственности на программиста за вред, причинённый такими системами. В работе анализируются свойства искусственного интеллекта, которые могут влиять на степень общественных деяний, совершенных с его использованием. Среди таких свойств автор выделяет автономность как способность интеллектуальных систем действовать и принимать решения независимо от человека. Другим характерным свойством современных систем искусственного интеллекта является непрозрачность. Непрозрачность может проявляться как недоступность алгоритмов, исходного кода, обученной нейронной сети или её архитектуры в связи с их правовой охраной как интеллектуальной собственности или государственной тайны. Непрозрачность обусловлена тем, что понимание программного кода и архитектуры систем искусственного интеллекта требует специальных знаний и навыков. Кроме того, понимание работы некоторых систем лежит за гранью человеческих возможностей.

¹Роман Игоревич Дремлюга, кандидат юридических наук, доцент Юридической школы, Дальневосточный федеральный университет, г. Владивосток, Россия.

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

Анализ показывает, что использование систем искусственного интеллекта повышает степень общественной опасности преступного деяния. Во-первых, использование интеллектуальных систем создает у преступника чувство безопасности при совершении преступлений посредством искусственного интеллекта. Между злоумышленником и потерпевшим есть своеобразный буфер в виде компьютерной программы. Преступник для совершения общественно опасного деяния не контактирует с жертвой. Анонимность и обезличенность при использовании интеллектуальной системы преступником позволяют выдать себя за другого человека, скрыться от правосудия, остаться вне общественного порицания и осуждения.

Ключевые слова: искусственный интеллект, киберправо, автономные системы, информационные технологии, сквозные технологии, прорывные технологии, киберпреступления, преступления в сфере компьютерной информации, уголовное право, уголовный закон, общественная опасность, степень общественной опасности, средство совершения преступления, уголовный кодекс, отягчающие обстоятельства, право информационных технологий, цифровая экономика, цифровая трансформация, информационное общество, новый технологический уклад, право и этика искусственного интеллекта.

Для цитирования: Дремлюга Р. И. Использование искусственного интеллекта в преступных целях: уголовно-правовая характеристика // Азиатско-Тихоокеанский регион: экономика, политика, право. 2021. № 3. С. 153–165. <https://doi.org/10.24866/1813-3274/2021-3/153-165>.

Original article

APPLICATION OF ARTIFICIAL INTELLIGENCE FOR CRIMINAL PURPOSES FROM CRIMINAL LAW PERSPECTIVE

Dremluga Roman I.¹, Far Eastern Federal University, Vladivostok, Russia
E-mail: dreamluck@yandex.ru

Abstract. Artificial Intelligence is actively used in many areas of human life. The use of artificial intelligence systems increases the efficiency of activities, reduces costs, and increases productivity. It is assumed that such a productive tool will soon be actively used for criminal purposes. The article analyzes the concept of "artificial intelligence" and its distinctive characteristics. The author concludes that modern artificial intelligence systems are trained, not programmed, which reduces the feasibility of imposing liability on

¹ *Roman I. Dremluga*, Candidate of Law, Associate Professor of the School of Law, Far Eastern Federal University, Vladivostok, Russia.

the programmer for the damage caused by such systems. The paper analyzes the properties of artificial intelligence, which may affect the degree of social acts committed with it. Among such properties, the author highlights autonomy as the ability of intelligent systems to act and make decisions independently of humans. Opacity is yet another characteristic property of modern artificial intelligence systems. It can manifest itself as inaccessibility of algorithms, source code, trained neural networks, or architecture due to their legal protection as intellectual property or state secrets. Opacity is contingent on the fact that understanding the program code and architecture of artificial intelligence systems require special knowledge and skills. In addition, understanding the work of some systems is beyond human capabilities.

The analysis shows that artificial intelligence systems increase the degree of public danger of a criminal act. First, intelligent systems create a sense of security for the criminal when committing crimes through AI. A computer program serves as a buffer between the perpetrator and the victim. The perpetrator has no contact with the victim to commit a socially dangerous act. Anonymity and impersonality when using an intelligent system by a criminal allow him/her to pass off as a different person, hide from justice, and remain outside of public censure and condemnation.

Keywords: artificial intelligence, cyber law, autonomous systems, information technology, end-to-end technology, breakthrough technology, cybercrime, computer information crime, criminal law, criminal law, public danger, degree of public danger, means of crime, criminal code, aggravating circumstances, information technology law, digital economy, digital transformation, information society, new technological way, law and ethics of artificial intelligence.

For citing: Dremliuga R. I. Application of Artificial Intelligence for Criminal Purposes from Criminal Law perspective // PACIFIC RIM: Economics, Politics, Law. 2021. No. 3. 153–165. <https://doi.org/10.24866/1813-3274/2021-3/153-165>.

Искусственный интеллект является одной из наиболее многообещающих технологий. С помощью интеллектуальных компьютерных программ можно заменить человека буквально во всех сферах. Внедрение данной технологии неминуемо ведет к кардинальным изменениям в общественной, экономической и военно-политической сфере. Активно искусственный интеллект используется злоумышленниками для более эффективного достижения преступных целей. Так как применение данной перспективной технологии для совершения преступлений отражается на качественных характеристиках преступного деяния, необходимо оценить степень общественной опасности деяний, совершаемых с помощью искусственного интеллекта.

Для анализа того, как влияет использование искусственного интеллекта на степень общественной опасности преступления, необходимо понять, чем данная ком-

пьютерная технология отличается от других. Так как термин относится к компьютерным наукам, большинство определений можно встретить в технической литературе. Так, некоторые зарубежные специалисты определяют искусственный интеллект как способность машины (технического средства) имитировать интеллектуальное поведение (англ. AI is the capability of a machine to imitate intelligent behavior) [1, с. 23]. До возникновения технологии ИИ такое поведение в основном ассоциировалось только с человеком. Речь о деятельности, которая требует интеллектуальных усилий, к ним могут относиться самые разные формы от творчества до распознавания и анализа текстов. В настоящее время трудно найти сферу, где не используется искусственный интеллект.

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, причём способ поведения зависит не только от текущего состояния информационных входов, но также и от предыдущих состояний системы» [2, с. 67]. В данном определении выделяются признаки автономности и самодетерминированности, которые отличают системы искусственного интеллекта от большинства других компьютерных систем.

Термин искусственный интеллект используется для обозначения как определенных математических методов и алгоритмов, так и для компьютерных систем, реализованных на их основании. Также дефиниция используется как наименование области компьютерных наук, в рамках которой изучаются способы построения компьютерных систем, способных к разумному поведению.

В последнее время наиболее распространённым подходом в разработке искусственного интеллекта являются глубокие нейронные сети (англ. Deep Neural Network). При использовании данного метода, по сути, с помощью компьютера имитируется работа нейронных сетей живых организмов. Глубокие нейронные сети, в отличие от других методов, обучаются действовать в непредсказуемой среде, где количество вариантов поступающих входных данных не ограничено заранее определённым набором [3, с. 7–10]. Подобные системы способны успешно водить автомобиль, поддерживать беседу, заниматься творчеством и т.д.

На практике доказано, что многие задачи искусственный интеллект решает более эффективно, чем человек. Например, искусственный интеллект, основанный на глубоких нейронных сетях, выиграл у нескольких мировых чемпионов по шашкам Го. До этого события считалось, что такое превосходство компьютера над человеком невозможно, так как ходы данной игры невозможно просчитать простым перебором. Количество возможных комбинаций в данной игре больше, чем атомов во вселенной. Так как в системе была использована искусственная нейронная сеть, она не была запрограммирована в буквальном смысле. Искусственный интеллект обу-

чился играть на таком высоком уровне, сыграв множество партий с самим собой. Для достижения полного превосходства ИИ пришлось сыграть 29 млн партий [4, с. 354–359].

Таким образом, в процессе разработки искусственных нейронных сетей они не программируются, а обучаются либо на предоставляемых учебных данных, либо взаимодействуя с подобными себе системами. Программист необходим на этапе выбора архитектуры нейронной сети или проверки результатов обучения. Неправильное понимание процесса создания и характеристик работы систем искусственного интеллекта ведёт к затруднению в разработке системы правовых норм, регулирующих отношения по поводу использования систем искусственного интеллекта.

Некоторые российские исследователи предполагают, что алгоритм действий робота полностью определяется человеком, даже если речь идет об искусственном интеллекте и самообучаемых нейронных сетях [5, с. 51]. Данный тезис по отношению к современным системам искусственного интеллекта зачастую неверен, так как предсказать, как будет вести себя нейронная сеть, для определённого набора данных можно лишь с некоторой долей вероятности.

Другие авторы считают, что необходимо возложить всю ответственность за последствия действий систем ИИ на разработчика (программиста). При этом важнейшим вопросом использования интеллектуальных компьютерных систем является правовая регламентация «вопроса об ошибках при программировании и их последствиях» [6, с. 17]. Таким образом, многие исследователи не понимают одно из основных отличий современных систем искусственного интеллекта от традиционных компьютерных систем: автономность.

Существенно значимыми элементами автономности от человека, являются по мнению некоторых исследователей:

- субъектность (в том числе – автономность как интеллектуального агента, самостоятельность и самореферентность в самообучении и в выработке и принятии решений);
- когнитивная и адаптационная автономность (способность получать информацию извне и менять свое состояние в соответствии с поступающими данными);
- 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 [7, с. 105].

В связи с высокой автономностью некоторых систем искусственного интеллекта зарубежные исследователи-правоведы предлагают признать искусственный интеллект субъектом уголовного права. В некоторых исследованиях проводится

аналогия с уголовной ответственностью юридических лиц, которая привычна для правовых систем многих стран мирового сообщества. Предлагаются даже аналогичные виды наказаний, применимых к системам искусственного интеллекта. В качестве аналога смертной казни можно использовать стирание программы искусственного интеллекта без возможности восстановления, а в качестве лишения свободы – отключение компьютера от сети или его выключение на определённый срок [8].

Данная позиция разделяется некоторыми российскими исследователями, которые считают, что усложнение, децентрализация, автономизация технологий искусственного интеллекта создают ряд проблем для человека, осуществляющего контроль над такими технологиями: человек, даже управляющий системой ИИ, не всегда способен полностью контролировать все действия и реакции системы, а тем более предугадать её поведение [9, с. 99–100]. Несмотря на относительную автономность систем ИИ, считаем, что уголовная ответственность систем искусственного интеллекта возможна только в странах, где в уголовно-правовой традиции распространено объективное вменение. В российском уголовном праве, где объективное вменение напрямую запрещено уголовным законом (ч. 2 ст. 5 УК РФ), уголовная ответственность систем искусственного интеллекта недопустима.

Кроме того, одним из характерных свойств современных систем искусственного интеллекта является непрозрачность. Некоторые зарубежные исследователи искусственного интеллекта считают, что непрозрачность может проявляться в нескольких смыслах. Во-первых, непрозрачность как недоступность системы на основании закона, когда речь идёт о недоступности алгоритмов, исходного кода, обученной нейронной сети или её архитектуры в связи их правовой охраной как интеллектуальной собственности или государственной тайны [10, с. 3]. Использование той или иной системы искусственного интеллекта даёт преимущество отдельным компаниям на рынке или целым государствам.

Во-вторых, непрозрачность обусловлена тем, что понимание программного кода и архитектуры систем искусственного интеллекта – это специализированный навык, который многим не доступен. Таким образом, даже если законодательно открыть доступ к исходному коду интеллектуальных систем, не так много людей смогут понять, как они работают. Кроме того, такие специалисты крайне востребованы на рынке и имеют высокую оплату за применение своих знаний. В связи с этим привлечь специалистов для анализа работы системы или выявления ошибок разработчика достаточно трудно.

Сложно осуществлять общественный контроль корректности работы таких систем. Для понимания работы надо как минимум знать синтаксис языков программирования, таких как C или Python, которые сильно отличаются от человеческих языков [10, с. 4]. С архитектурой современных систем искусственного интеллекта,

например, нейронных сетей, всё ещё сложнее. Понимание их работы требует обширных математических знаний, архитектур сетей и характеристик данных, на которых обучалась система [3, с. 38].

Третий вид непрозрачности в некотором смысле непреодолим. Современные системы искусственного интеллекта становятся такими сложными, что выходят за пределы человеческого понимания. Например, система искусственного интеллекта может оперировать триллионами единиц в пространстве с тысячей измерений [10, с. 4]. В данном случае привлечение специалиста лишь поможет понять основные характеристики работы системы. Следует отметить, что сложность систем искусственного интеллекта с каждым годом только увеличивается, а значит, разрыв между возможностями человеческого разума и непрозрачностью систем растёт.

Обобщая вышесказанное, получается, что система искусственного интеллекта – это компьютерная система или программа, имитирующая один или несколько аспектов интеллектуального поведения, обладающая более высокой по сравнению с другими компьютерными системами или программами степенью самодетерминированности и независимости от воли разработчика или пользователя. Некоторые интеллектуальные системы способны к обучению и самообучению. Такие системы обладают определённой долей непрозрачности и непредсказуемости для разработчиков и лиц, их использующих.

Серьёзным вызовом для правового регулирования отношений по поводу применения систем искусственного интеллекта являются широкие возможности для его противоправного или преступного использования. Некоторые из возможностей «умных машин» заставляют по-новому посмотреть на целые отрасли и институты права.

Например, в рамках одного исследования была обучена глубокая нейронная сеть, которая на основе анализа всего 5 фотографий с сайта знакомств определяла персональные особенности человека. Так, нетрадиционная сексуальная ориентация определялась с точностью более девяноста процентов. С помощью обученной нейронной сети также определялись политические взгляды, уровень интеллекта и другие личные характеристики [11, с. 256]. Таким образом, стирается грань между частным и публичным, так как личная информация о персоне может быть «смоделирована» из открытых источников.

Некоторые исследователи говорят об исчезновении в скором времени такого понятия, как частная жизнь, так как все мы будем абсолютно открыты для интеллектуальных компьютерных систем. Следует отметить, что распространённость внедрения таких систем государствами и частными компаниями увеличилась в результате мировой пандемии коронавируса [12].

Особую угрозу представляет широкая распространённость транспортных автономных устройств, которые могут достигать любых точек на суше [13], водной среде [14] или в воздушном пространстве. Такие системы с «компьютерным мозгом» уже

сейчас активно используются в преступных целях. Так, беспилотные летательные аппараты (БЛА) активно применяются преступниками для перевозки и доставки наркотиков, а также других запрещенных к обороту вещей. Используемый в нелегальных целях летательный аппарат достигает цели по указанным координатам без непосредственного управления человеком, то есть в автономном режиме [20].

Крайне опасной видится перспектива применения автономного транспорта для осуществления террористических атак. Беспилотник может быть использован для доставки взрывчатых веществ и выступать самостоятельной поражающей единицей. Автомобили с водителем уже применялись террористическими группами для совершения атак в европейских странах. По мнению исследователей, при подготовке такой атаки потенциальный террорист-смертник может отказаться от совершения массового убийства или пойти в полицию, что является слабым местом при подготовке [15, с. 9–11]. Автономное транспортное средство в качестве орудия совершения теракта избавлено от этого недостатка и в то же время самостоятельно может достигнуть любой цели.

Способность систем искусственного интеллекта имитировать интеллектуальное поведение человека означает возможность для преступников выдавать себя за другую личность. Такое противоправное деяние в юридической литературе стран англосаксонского права обозначается как кража личности (англ. – identity theft). Нередко интеллектуальные системы используются для совершения преступлений [16; 17]. Например, с помощью программ, генерирующих голосовые сообщения, похожие на речь какого-либо лица, совершаются мошеннические действия [21]. А посредством имитации видеоизображений отдельных лиц у мошенников получилось обмануть умные системы оплаты [22].

Специально обученные системы искусственного интеллекта способны имитировать аудиовизуальные изображения каких-либо лиц без их согласия с высокой степенью реалистичности. Широкая доступность и низкие требования к оборудованию позволяют создать подделку даже в домашних условиях [18]. Аудиовизуальные имитации могут применяться для совершения целого спектра деяний: от общения от имени другого лица в мессенджерах до обхода биометрических систем.

В условиях глобальной пандемии COVID-19, когда значительная часть социальной активности перешла в киберпространство, кража электронной личности означает, что появилась возможность полностью подменить жертву фальшивой личностью. Таким образом, интеллектуальные системы могут и активно используются преступниками для совершения общественно опасных деяний. Это могут быть преступления самых разных категорий – от преступлений в сфере экономики до деяний против общественной безопасности и общественного порядка.

Анализ показывает, что использование систем искусственного интеллекта повышает степень общественной опасности преступного деяния. Во-первых, исполь-

зование интеллектуальных систем создаёт у преступника чувство безопасности при совершении преступлений посредством ИИ. Между злоумышленником и потерпевшим есть своеобразный буфер в виде компьютерной программы. Преступник для совершения общественно опасного деяния не контактирует с жертвой. Анонимность и обезличенность при использовании интеллектуальной системы позволяют преступнику выдать себя за другого человека, скрыться от правосудия, остаться вне общественного порицания и осуждения.

Использование интеллектуальных систем повышает эффективность, снижает издержки, минимизирует риски и позволяет повысить охват преступной деятельностью. Преступный результат достигается без активного вовлечения преступника. Обучив и запустив систему, можно, не прилагая усилий, пользоваться результатами её работы.

Автоматизации может быть подвергнута преступная деятельность, потенциально имеющая глобальный охват. Например, распространенный способ мошенничества «нигерийские письма» может быть легко автоматизирован без потери эффективности. Суть метода обмана в том, что преступник рассылает текст сообщения, предлагая под тем или иным ложным предлогом перевести на счет мошенника деньги. «Как правило, мошенники просят у получателя письма помощи во многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются определённые суммы денег под предлогом оформления сделок, залогов, уплаты сборов и т.д.» [19]. Эффективность рассылки одного и того же или похожих писем достаточно низка, во-первых, о появлении нового способа для отъёма денег быстро становится известно общественности, а во-вторых, текст не адаптирован под конкретную жертву, то есть не учитывает её культуру, язык, слабости и предпочтения.

При рассылке «нигерийских писем» через электронную почту или в социальных сетях искусственный интеллект сможет из общедоступных данных получить сведения о слабости и особенностях потенциальной жертвы. Соответственно адаптированные к конкретному человеку сообщения мошеннического характера будут более эффективны. Например, для любителя собак ИИ будет просить деньги на помощь собакам, а для борцов против климатических изменений – средства на новую акцию. При этом интеллектуальная система может даже самообучаться и адаптировать стилистику в зависимости от результатов переписки.

Также стоит отметить среди характеристик машин «интеллектуальность». В примере, приведённом выше, речь о возможности имитации деятельности человека, которая является признаком интеллектуального поведения (возможность коммуницировать с человеком и манипулировать им). Компьютерный интеллект способен превосходить человека во многих аспектах как, например, определение точного психологического портрета или склонностей собеседника. То есть исполь-

зование интеллектуальных систем для совершения преступления более общественно опасно из-за свойства интеллектуальности подобных систем.

Применение систем искусственного интеллекта существенно облегчает и даже упрощает процесс совершения преступления. Интеллектуальное программное или аппаратное обеспечение компенсирует отсутствие специальных знаний у преступника, а также значительно расширяет его возможности.

Использование искусственного интеллекта увеличивает степень общественной опасности преступного деяния и должно повлечь более строгие меры ответственности. Применение рассматриваемого средства совершения преступления должно быть сформулировано в качестве отягчающего обстоятельства общей части Уголовного Кодекса Российской Федерации. В статью 63 УК РФ следует добавить пункт «с», сформулированный как **«совершение преступления посредством систем искусственного интеллекта»**.

Кроме того, предлагается ввести квалифицирующий признак **«совершённое посредством систем искусственного интеллекта»** в статьи Главы 28 «Преступления в сфере компьютерной информации» Уголовного кодекса Российской Федерации.

Список литературы

1. Padhy, N. P. Artificial intelligence and intelligent systems 3 / N. P. Padhy. – Oxford : Oxford University Press, 2005. 632 p.
2. Якушев, Д. И. Об определении искусственного интеллекта // Региональная информатика и информационная безопасность : сборник трудов. – Санкт-Петербург : Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления, 2016. – С. 67–69.
3. Николенко, С. Глубокое обучение / С. Николенко, А. Кадури, Е. Архангельская. – Санкт-Петербург : Питер, 2020. – 480 с.
4. Mastering the game of Go without human knowledge / D. Silver, J. Schrittwieser, K. Simonyan [et al.] // Nature. – 2017. – Vol. 550 (7676). – P. 354–359.
5. Васильев, А. А. Правовое регулирование робототехники и искусственного интеллекта в Европейском Союзе / А. А. Васильев, Ж. И. Ибрагимов // Российско-азиатский правовой журнал. – 2019. – № 1. – С. 50–54.
6. Васильев, А. А. Искусственный интеллект и право: проблемы, перспективы / А. А. Васильев, Ю. В. Печатнова // Российско-азиатский правовой журнал. – 2020. – № 2. – С. 14–18.
7. Понкин, И. В. Искусственный интеллект с точки зрения права / И. В. Понкин, А. И. Редькина // Вестник Российского университета дружбы народов. Серия : Юридические науки. – 2018. – Т. 22, № 1. – С. 91–109.
8. Hallevy, G. When Robots kill: Artificial intelligence under criminal law / G. Hallevy. – Boston : Northeastern University, 2013. – 244 p.

9. Хисамова, З. И. Сущность искусственного интеллекта и проблема определения правосубъектности / З. И. Хисамова, И. Р. Бегишев // Вестник Московского государственного областного университета. Серия : Юриспруденция. – 2020. – № 2. – С. 96–106.
10. Burrell, J. How the machine 'thinks:' understanding opacity in machine learning algorithms // Big Data & Society. – 2016. – January – June. – P. 1–12.
11. Kosinski, M. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images / M. Kosinski, Y. Wang // Journal of Personality and Social Psychology. – 2018. – Vol. 114 (2). – P. 246–257.
12. Lee, T. Tracing surveillance and auto-regulation in Singapore: «smart» responses to COVID-19 / T. Lee, H. Lee // Media International Australia. – 2020. – Vol. 177 (1). – P. 47–60.
13. Дремлюга, Р. И. Регулирование тестирования и использования беспилотного автотранспорта: опыт США / Р. И. Дремлюга, А. В. Крипакова, А. А. Яковенко // Журнал зарубежного законодательства и сравнительного правоведения. – 2020. – № 3 (82). – С. 68–85.
14. Гаврилов, В. В. Актуальные вопросы международно-правового регулирования плавания морских судов без экипажа / В. В. Гаврилов, Р. И. Дремлюга // Московский журнал международного права. – 2020. – № 2. – С. 65–76.
15. Miller, V. I Did my bit': Terrorism, tarde and the vehicle ramming attack as an imitative event / V. Miller, K. J. Hayward // British Journal of Criminology. – 2019. – Vol. 59 (1). – P. 1–23.
16. Watney, M. M. Artificial intelligence and its' legal risk to cybersecurity // European Conference on Information Warfare and Security, ECCWS, 2020-June. – [S. l.], 2020. – P. 398–405.
17. Young, O. R. Meeting cyber age needs for governance in a changing global order / O. R. Young, J. Yang, D. Guttman. – DOI 10.3390/su12145557 // Sustainability (Switzerland). – 2020. – Vol. 12 (14). – Art. no. 5557 [17 p.].
18. Deepfake detection algorithms: a meta-analysis / S. Zotov, R. Dremluga, A. Borshevnikov, K. Krivosheeva // ACM International Conference Proceeding Series. Ser. 2 : «SSPS 2020 – 2020 2nd Symposium on Signal Processing Systems». – Guangdong, 2020. – P. 43–48.
19. Фадина, Ю. П. Уголовно-правовая характеристика мошенничества в сети интернет // Вестник Югорского государственного университета. – 2017. – № 1–2 (44). – С. 117–121.
20. Drug delivery drone crashes in Mexico. – URL: <https://www.bbc.com/news/technology-30932395> (дата обращения: 07.05.2021).

21. ИИ помог мошенникам имитировать голос CEO компании и похитить 220 000 евро // Хакер. – URL: <https://haker.ru/2019/09/05/voice-deepfake/> (дата обращения: 07.05.2021).

22. Аферисты сумели украсть \$76 млн благодаря технологии Deepfake. – URL: <https://news.rambler.ru/internet/46154575/> (дата обращения: 07.05.2021).

References

1. Padhy N. P. *Artificial intelligence and intelligent systems* 3. Oxford: Oxford University Press. 2005. 632 p.
2. Yakushev D. I. Ob opredelenii iskusstvennogo intellekta [On the definition of artificial intelligence]. In: *Regional'naya informatika i informatsionnaya bezopasnost': sbornik trudov* [Regional informatics and information security: Proceedings]. – St. Petersburg: St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems, 2016, pp. 67–69.
3. Nikolenko S., Kadurin A., Arkhangel'skaya E. *Glubokoe obuchenie* [Deep learning]. – St. Petersburg: Peter, 2020. 480 p.
4. 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, vol. 550 (7676), pp. 354–359.
5. Vasiliev A. A., Ibragimov Zh. I. Pravovoe regulirovanie robototekhniki i iskusstvennogo intellekta v Evropeiskom Soyuze [Legal regulation of robotics and artificial intelligence in the European Union]. *Rossiisko-aziatskii pravovoi zhurnal*, 2019, no. 1, pp. 50–54.
6. Vasiliev A. A., Pechatnova Yu. V. Iskusstvennyi intellekt i pravo: problemy, perspektivy [Artificial intelligence and law: problems, prospects]. *Rossiisko-aziatskii pravovoi zhurnal*, 2020, no. 2, pp. 14–18.
7. Ponkin I. V., Redkina A. I. Iskusstvennyi intellekt s tochki zreniya prava [Artificial intelligence from the point of view of law]. *Vestnik Rossiiskogo universiteta družby narodov. Seriya: Yuridicheskie nauki*, 2018, vol. 22, no. 1, pp. 91–109.
8. Hallevy G. *When Robots kill: Artificial intelligence under criminal law*. Boston: Northeastern University, 2013. 244 p.
9. Khisamova Z. I., Begishev I. R. Sushchnost' iskusstvennogo intellekta i problema opredeleniya pravosub'ektnosti [The essence of artificial intelligence and the problem of determining legal personality]. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Yurisprudentsiya*, 2020, no. 2, pp. 96–106.
10. Burrell J. How the machine 'thinks:' understanding opacity in machine learning algorithms. *Big Data & Society*, 2016, January – June, pp. 1–12.

11. Kosinski M., Wang Y. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*, 2018, vol. 114 (2), pp. 246–257.
12. Lee T., Lee H. Tracing surveillance and auto-regulation in Singapore: «smart» responses to COVID-19. *Media International Australia*, 2020, vol. 177 (1), pp. 47–60.
13. Dremlyuga R. I., Kripakova A. V., Yakovenko A. A. Regulirovanie testirovaniya i ispol'zovaniya bespilotnogo avtotransporta: opyt SShA [Regulation of testing and use of unmanned vehicles: the US experience]. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya*, 2020, no. 3 (82), pp. 68–85.
14. Gavrilov V. V., Dremlyuga R. I. Aktual'nye voprosy mezhdunarodno-pravovogo regulirovaniya plavaniya morskikh sudov bez ekipazha [Topical issues of international legal regulation of navigation of sea vessels without a crew]. *Moskovskii zhurnal mezhdunarodnogo prava*, 2020, no. 2, pp. 65–76.
15. Miller V., Hayward K. J. I Did my bit': Terrorism, tarde and the vehicle ramming attack as an imitative event. *British Journal of Criminology*, 2019, vol. 59 (1), pp. 1–23.
16. Watney M. M. Artificial intelligence and its' legal risk to cybersecurity. *European Conference on Information Warfare and Security, ECCWS, 2020-June*, 2020, pp. 398–405.
17. Young O. R., Yang J., Guttman D. Meeting cyber age needs for governance in a changing global order. *Sustainability (Switzerland)*, 2020, vol. 12 (14), art. no. 5557. DOI: 10.3390/su12145557.
18. Zotov S., Dremlyuga R., Borshevnikov A., Krivosheeva K. Deepfake detection algorithms: a meta-analysis. ACM International Conference Proceeding Series. 2. «SSPS 2020 – 2020 2nd Symposium on Signal Processing Systems». Guangdong, 2020, pp. 43–48.
19. Fadina Yu. P. Uголовно-правовая характеристика moshennichestva v seti internet [Criminal and legal characteristics of fraud on the Internet]. *Vestnik Yugorskogo gosudarstvennogo universiteta*, 2017, no. 1–2 (44), pp. 117–121.
20. *Drug delivery drone crashes in Mexico*. Available at: <https://www.bbc.com/news/technology-30932395> (accessed 05 July 2021).
21. AI helped scammers imitate the voice of the company's CEO and steal 220,000 euros. *Hacker*. Available at: <https://xakep.ru/2019/09/05/voice-deepfake/> (accessed 05 July 2021). (In Russian).
22. *Swindlers managed to steal \$ 76 million thanks to Deepfake technology*. Available at: <https://news.rambler.ru/internet/46154575/> (accessed 05 July 2021). (In Russian).