Научная статья
УДК 341.9; 343.9.018.3
EDN USOFCJ
DOI 10.17150/2500-1442.2023.17(1).5-12

ПРЕСТУПНЫЕ ПОСЯГАТЕЛЬСТВА НА СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА

Р.И. Дремлюга, А.И. Коробеев
Дальневосточный федеральный университет, г. Владивосток, Российская Федерация

Информация о статье

Дата поступления
10 января 2023 г.

Дата принятия в печать
21 февраля 2023 г.

Дата онлайн-размещения
13 марта 2023 г.

Ключевые слова

Искусственный интеллект; преступления в сфере компьютерной информации; состязательные атаки; неправомерный доступ; вредоносная программа; умные города

Финансирование

Исследование выполнено при финансовой поддержке ДВФУ (программа стратегического академического лидерства «Приоритет-2030»: центр цифрового развития)

Аннотация. Искусственный интеллект, по мнению большинства специалистов, — это технология, которая определяет наше настоящее и будущее. Интеллектуальные технологии все чаще используются в критически значимых для социума сферах, таких как безопасность, энергетика, медицинская, правоохранительная и судебная деятельность, а также транспорт. Система искусственного интеллекта — это какой-либо исполняемый программный код или коэффициенты модели, которые при подаче на вход определенных данных заставляют систему выдавать определенный результат. Как и любая другая компьютерная информация, система искусственного интеллекта может стать предметом преступного посягательства. В статье рассмотрены посягательства на системы искусственного интеллекта, за которые уже предусмотрена уголовная ответственность в современном российском законодательстве. Также авторы выявляют такой вид посягательств на интеллектуальные системы, как состязательные атаки. Их суть заключается в том, что пользователь, зная особенности разработки и создания искусственного интеллекта, намеренно подает на вход системы данные, которые приводят к ее некорректной работе. Такие способы воздействия на интеллектуальные системы могут не содержать признаки преступлений, за которые уже предусмотрена уголовная ответственность современным российским законодательством. В статье доказывается, что подобные деяния могут иметь высокую степень общественной опасности, достаточную для их криминализации. Авторы приходят к выводу, что существующее российское уголовное законодательство не охватывает все способы общественно опасных посягательств на системы искусственного интеллекта. Высокая степень общественной опасности состязательных атак подразумевает необходимость признания преступными посягательства на системы искусственного интеллекта посредством воздействия на компьютерные системы без использования вредоносных программ и неправомерного доступа.

Original article

CRIMINAL INFRINGEMENT ON ARTIFICIAL INTELLIGENCE SYSTEMS: A CRIMINAL LAW DESCRIPTION

Roman I. Dremliuga, Alexander I. Korobeev
Far Eastern Federal University, Vladivostok, the Russian Federation

Article info

Received
2023 January 10

Accepted
2023 February 21

Available online
2023 March 13

Abstract. Most specialists agree that artificial intelligence (AI) is the technology that defines our present and future. Intelligent technologies are becoming increasingly common in critical social spheres, such as security, energy, medicine, law enforcement and judiciary, as well as transportation. An AI system is an executable program code or coefficients of a model that, given certain input data, make the system produce a certain result. As any other computer information, an AI system may become an object of criminal infringements. The authors study infringements on AI systems that incur criminal liability under the current Russian legislation. They also single out such a type of infringements on AI systems as adversarial attacks. These attacks are cases when a user, knowing about the specifics of developing and creating an

ISSN 2500-1442

Keywords

Artificial intelligence; information technology crimes; adversarial attacks; illegal access; malware; smart cities

Acknowledgements

Research was supported by the Far Eastern Federal University (Program of Strategic Academic Leadership «PRIORITY 2030»: Digital Development Center)

AI system, intentionally feeds it data that lead to the incorrect functioning of this system. Such methods of interfering with intelligent systems may not contain formal attributes of offences that are criminally punishable under current Russian legislation. The authors of the article prove that such actions may have a high degree of public danger, which is sufficient for their criminalization. They conclude that current Russian criminal legislation does not encompass all methods of publicly dangerous infringements on AI systems. A high degree of public danger associated with adversarial attacks means that they should be recognized as criminal infringements on AI systems committed through influencing them without the use of malware or unauthorized access.

В настоящее время искусственный интеллект (ИИ) используется во всех сферах нашей жизни. Он помогает выбрать музыку или видео, совершить покупку, его технология способна управлять транспортными средствами [1] и ставить более точный диагноз, чем человек [2; 3]. В последние несколько лет благодаря накоплению огромных объемов данных и достижениям в методологии глубокого обучения нейросетей системы машинного обучения достигли невероятных результатов в выполнении большого разнообразия задач. Стремительное развитие наблюдается в решении задач понимания человеческой речи, распознавания изображений, анализа настроений, стратегического планирования игр и многих других. Например, в медицине модели на основе искусственных нейронных сетей используются для диагностики различных заболеваний, таких как рак груди и т.д., на основе данных о симптомах и снимков с различного вида врачебного оборудования.

ИИ можно определить как способность ИТ-системы имитировать интеллектуальное поведение [4]. До распространения технологии ИИ подобное поведение в основном ассоциировалось с людьми. Речь не о банальной автоматизации, а о способности выполнять функции и решать задачи, которые требуют вовлечения интеллектуальных ресурсов. К данному классу задач относятся самые разные формы деятельности: от творчества до распознавания и анализа текстов.

Термин «искусственный интеллект» обозначает как математические методы и алгоритмы с определенными свойствами, так и ИТ-системы, реализованные на их основании. Дефиниция также используется как название отрасли компьютерных наук, в рамках которой изучаются приемы построения и обучения компьютерных систем, способных к разумному поведению.

Особенности систем ИИ создают трудности для правовой регламентации общественных отношений по поводу их разработки, внедрения и применения. Многие современные модели сталкиваются с недостатком прозрачности и интерпретируемости, что является серьезным препятствием во многих приложениях, например в финансах, судебной системе и здравоохранении, где визуализация, интерпретация и объяснение являются обязательным условием внедрения систем ИИ [5]. Эта проблема характерна для современных интеллектуальных методов, к примеру глубоких нейронных сетей, и была не такой явной для существовавших ранее систем.

Еще одним проблемным для правовой политики свойством современных систем ИИ является умение имитировать интеллектуальное поведение человека. В данном контексте одна из самых обсуждаемых проблем, связанных с распространением ИИ, которая, по мнению экспертов, значительно повлияет на правовую политику государств, — это технологическая безработица. Тема повсеместной замены людей интеллектуальными машинами в различных сферах экономической деятельности широко обсуждается в научной и публицистической литературе. Потенциальный эффект цифровизации экономики с использованием автономных роботов и ИИ на рынке труда подробно описан и часто сравнивается с наихудшими кризисами, которые переживало общество. Внедрение систем ИИ, кажущееся сейчас экономически и социально обоснованным, в будущем угрожает ныне существующему общественному укладу в целом [6–8].

В условиях уменьшения возможностей качественной занятости главной социальной проблемой становится неизбежная маргинализация и фрагментация среднего класса. При этом упомянутая общественная группа является опорой современного миропорядка. Средний класс — основной налогоплательщик, и, следовательно, возможности современного государства по финансированию социальных расходов сокращаются пропорционально количеству безработных в данной группе [9].

Государства могут столкнуться с тотальной безработицей и ростом разрыва в доходах, поскольку многие трудовые функции будут выполняться роботами и интеллектуальными программами. При этом контроль над практически бесплатной рабочей силой будет осуществляться небольшой социальной группой людей. В дальнейшем это потребует облегчения бремени безработицы за счет лучшего перераспределения доходов и льгот. Некоторые авторы предлагают кардинальным образом решить данную проблему, пересмотрев правовую политику в сфере социальных гарантий и внедрив практику безусловных выплат всем безработным.

Уголовное право охраняет от преступных посягательств общественные отношения, которые регулируются нормами других отраслей права. По поводу использования систем ИИ также сложился комплекс общественных отношений. Эти отношения могут входить в объект ряда преступных посягательств.

Система ИИ — это компьютерная информация (программный код и коэффициенты модели), которая обладает определенными характеристиками. Также система ИИ — это какой-либо исполняемый программный код или коэффициенты модели, которые при подаче на вход определенных данных заставляют систему выдавать определенный результат. Как и любая другая компьютерная информация, система ИИ может стать мишенью преступника.

В качестве предмета преступления система ИИ может выступать при неправомерном доступе к компьютерной информации (ст. 272, ч. 2 ст. 274.1 УК РФ). «Неправомерный доступ» в российском уголовном законодательстве означает, что лицо, нарушив установленный порядок доступа, с помощью технических средств проникло в хранилище компьютерной информации, что привело к ее уничтожению, блокированию, модификации либо копированию.

Согласно позиции Верховного Суда РФ, компьютерная информации должна обладать определенными свойствами. Так, Пленум Верховного Суда РФ в своем постановлении от 15 декабря 2022 г. № 37 предписал, что под охраняемой законом компьютерной информацией в контексте ст. 272 УК РФ подразумевается та, «для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение»[1]. Другим видом является та информация, для которой ее обладателем «установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности»[2].

Хотя позиция Верховного Суда небесспорна, российские суды чаще всего придерживаются предписанной им логики. Таким образом, если программный код или модель ИИ относятся к перечисленным выше видам компьютерной информации, то проникновение в хранилище с такими данными, в результате которого наступит уничтожение, блокирование, модификация либо копирование компьютерной информации, будет квалифицированно по ст. 272 УК РФ. При этом при квалификации не учитывается, относится ли такая компьютерная информация к системе ИИ или обученной модели.

Специалистами доказано, что неправомерный доступ к некоторым системам ИИ создает серьезные риски. Так, интеллектуальные системы являются сердцем автономных (беспилотных) автомобилей. Обещают, что такой транспорт изменит уровень безопасности и комфорта перевозок. Предполагается, что беспилотные автомобили будут подключены к различным внешним системам и использовать передовые встроенные системы для восприятия окружающей среды и принятия интеллектуальных решений. Тем не менее, по словам специалистов, такие автомобили уязвимыми к различным кибератакам, которые могут иметь катастрофические последствия. Атаки на автомобильные системы уже участились в современных транспортных средствах и, как ожидается, станут более распространенными при внедрении автономных транспортных средств. Таким образом, существует необходимость усиления уголовно-правовой охраны отношений по поводу безопасного использования ИИ в автономном автотранспорте. Особенно когда речь идет о защите от неправомерного доступа [10].

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верхов. Суда РФ от 15 дек. 2022 г. № 37 // СПС «КонсультантПлюс».

[2] Там же.

Степень общественной опасности преступлений, связанных с неправомерным доступом к интеллектуальным системам, также возрастает, когда ИИ используется в сфере медицины. В настоящий момент интеллектуальные системы применяются не только для диагностики заболеваний, приводящих к летальному исходу, но и для назначения лечения при таких болезнях. Вмешательство хакера может не просто причинить смерть или кардинально повлиять на здоровье одного человека, а привести к серьезным последствиям для большой группы людей. Так, системы ИИ внедряются в медицинских учреждениях для выявления злокачественных опухолей в различных органах человека [11; 12]. Также ИИ может использоваться в других значимых сферах — судебной [13], правоохранительной [14], финансовой [15]. Применение интеллектуальных систем там, где от них существенно зависят жизнь, здоровье, обеспечение основных прав и достаток людей, подтверждает высокую степень опасности неправомерного доступа к ИИ.

Интеллектуальные системы могут быть и частью критической информационной инфраструктуры (КИИ). С технической точки зрения объектом КИИ является элемент информационной инфраструктуры, от которого сильно зависят другие составляющие инфраструктуры. Надлежащее функционирование КИИ необходимо для удовлетворения потребностей больших групп людей и критично для обеспечения безопасности общества и государства. Такая инфраструктура может обрабатывать, хранить или передавать огромные объемы компьютерной информации. Поскольку обработка больших данных как раз и является одним из частых применений систем ИИ, то интеллектуальные компьютерные программы становятся частью КИИ.

В случае неправомерного доступа к системе ИИ, входящей в состав (являющейся частью) КИИ, преступное деяние должно быть квалифицировано по ч. 2 ст. 274.1 УК РФ. Несмотря на то что вред как конструктивный признак состава преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, в отличие от ст. 272 УК РФ, не конкретизирован, по мнению ряда авторов, системное толкование уголовно-правовых норм указывает на необходимость учета последствий неправомерного доступа к КИИ. Среди таких последствий: уничтожение, блокирование, модификация, копирование информации, содержащейся в КИИ, нейтрализация средств защиты указанной информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование КИИ [16].

На системы ИИ можно посягать и посредством вредоносных программ или иной компьютерной информации, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты. Если вредоносная программа создается, распространяется или используется против систем ИИ, то такое деяние должно быть квалифицировано по ст. 273 УК РФ. В случае если интеллектуальная система является частью или элементом КИИ, данное посягательство подлежит квалификации по ч. 1 ст. 274.1 УК РФ.

Также посягательства на системы ИИ (в отличие от других компьютерных систем) могут совершаться без неправомерного доступа и применения вредоносных программ. В настоящее время в компьютерной литературе все чаще обсуждается проблема состязательных атак на ИИ, когда интеллектуальным системам на вход подаются данные, которые злоумышленник намеренно скомпоновал так, чтобы заставить модель совершать ошибки [17]. Все чаще варианты таких атак обозначаются исследователями в критических сферах применения ИИ. Например, ряд аналитиков установил, что можно заставлять компьютерное зрение беспилотных автомобилей некорректно опознавать дорожные знаки путем незначительного их изменения. Насколько известно, такая атака осуществляется с помощью клейкой ленты или краски [18].

Примечательно, что нейронные сети (метод ИИ), демонстрирующие слабую устойчивость к такого рода посягательствам, применяются в различных областях. Среди них: системы биометрической безопасности, антивирусные и отслеживающие приложения и т.д. Так, коллектив исследователей кибербезопасности экспериментировал с обманом систем в так называемых умных магазинах. В рамках своего изыскания специалисты пришли к выводу, что разработанная ими небольшая наклейка, размещенная на любом товаре, купленном в таких магазинах, может привести к неправильной идентификации покупки и, как следствие, ошибочному (в пользу недобросовестного покупателя) взиманию платы за товар [19].

Суть состязательной атаки заключается в том, что пользователь, зная особенности разработки и создания ИИ, намеренно подает на вход системы данные, которые приводят к ее некорректной работе. Например, с помощью

определенным образом созданного принта на футболке можно заставить ИИ не находить лицо человека на изображении, а дорожный знак, искаженный специальным образом, может ввести в заблуждение компьютерное зрение беспилотного автомобиля [20–22].

Есть и задокументированные случаи состязательных атак, проведенных злоумышленниками для осуществления преступного замысла. Так, в Китае мошенники обманули всекитайскую банковскую систему распознавания лиц путем генерации искусственных изображений людей, которых система принимала за настоящих[3]. Данный вид посягательств может стать новым «неправомерным доступом», т.е. преступлением, которое предшествует другим общественно опасным деяниям, зачастую корыстной направленности.

Общественно опасное воздействие на системы ИИ иногда может содержать в себе признаки деяний, за которые уже установлена уголовная ответственность. Например, состязательная атака может иметь своей целью неправомерный доступ к какой-либо системе с последующим уничтожением, блокированием, изменением либо созданием копии компьютерной информации [23]. В данном случае деяние кибервзломщика, совершенное умышленно против системы ИИ, будет квалифицировано как преступление по ст. 272 УК РФ. Обман «умной» системы магазина, который описан ранее, следует квалифицировать как тайное хищение чужого имущества (ст. 158 УК РФ).

В то же время существуют способы воздействия на интеллектуальные системы, которые не содержат признаки перечисленных преступлений. Такие деяния могут иметь высокую степень общественной опасности. Системы ИИ выступают «цифровым мозгом» многих критически важных объектов. Правомерное использование подобных систем — это основа общественных отношений, формирующихся в настоящее время. Например, отдельные исследователи отмечают угрозу состязательных атак на информационную инфраструктуру «умных» городов. Концепция, которая возникла несколько лет назад, подразумевает, что инфраструктурой агломерации, экологией городской среды, безопасностью пространств управляет ИИ. Такие системы (или набор систем) внедрены в крупнейших мегаполисах мира. Степень самостоятельности (автономности) подобных ИИ варьируется от полностью автономных до рекомендательных для принятия решения людьми [24]. Также есть разброс того, насколько может быть опасна атака на подобные системы. Тем не менее состязательная атака может дестабилизировать или изменить эффективность работы целого города.

Состязательные атаки могут осуществляться и против систем обнаружения хакерских атак, а также других технологий, используемых в Промышленности 4.0 [25]. Умные роботы и сложные киберфизические системы для совместной работы машин и человека могут выступать предметом общественно опасного посягательства, осуществляемого посредством состязательной атаки. Технология состязательных атак может быть использована для вмешательства в работу систем, задействованных в критических промышленных объектах или в «умном» производстве [26]. Турбина самолета или узел электрогенерации с интегрированными цифровыми модулями интеллектуальной обратной связи могут быть отнесены к подобным системам.

Уязвимость перед состязательными атаками демонстрирует транспортная инфраструктура будущего. Речь идет об автономных транспортных средствах, системах контроля дорожного движения, программном обеспечении для предотвращения и детекции ДТП [27]. Разработчики методов обеспечения кибербезопасности автономного автотранспорта признают, что проблема состязательного хакинга не будет решена окончательно, поскольку непрерывно разрабатываются и выявляются новые методы неправомерного воздействия [21]. Состязательные атаки способны дестабилизировать дорожное движение без неправомерного доступа к компьютерным системам.

Умышленная состязательная атака даже без доступа к компьютерной информации или причинения имущественного вреда несет в себе существенную опасность для государства и общества. Во-первых, такие посягательства влекут недоверие к автономным системам, основанным на ИИ. Для государств вопрос скорости внедрения интеллектуальных систем неразрывно связан с их конкурентоспособностью, экономической эффективностью и безопасностью. Состязательные атаки как массовое явление могут вызвать отторжение использования технологий

[3] Взломана знаменитая китайская система распознавания лиц, заявленная как не преступная // Первый канал. URL: https://www.1tv.ru/news/2021-04-07/404459-vzlomana_znamenitaya_kitayskaya_sistema_raspoznavaniya_lits_zayavlennaya_kak_nepristupnaya.

у населения и замедлить переход к цифровой экономике конкретного государства.

Во-вторых, некорректная работа интеллектуальных систем дестабилизирует функционирование общества. ИИ используется практически во всех сферах жизни современного социума и может стать предметом посягательства состязательной атаки [28; 29]. В результате воздействия на систему ИИ, работа которой значима для общества, злоумышленник негативным образом влияет на нормальную жизнь большого количества людей. Например, состязательная атака на систему управления дорожным транспортом может быть неопасной с точки зрения повышения аварийности, но сделать нормальное дорожное движение практически невозможным.

Таким образом, существующее российское уголовное законодательство не охватывает все способы общественно опасных посягательств на системы ИИ. Высокая степень общественной опасности состязательных атак подразумевает необходимость признания преступными посягательства на системы ИИ посредством воздействия на компьютерные системы без использования вредоносных программ и неправомерного доступа.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Günsberg P.S. Automated vehicles — is a Dilution of Human Responsibility the Answer? / P.S. Günsberg // New Journal of European Criminal Law. — 2022. — № 13. — P. 439–451.

2. Artificial Intelligence in Cancer Research and Precision Medicine: Applications, limitations and Priorities to Drive Transformation in the Delivery of Equitable and Unbiased Care / C. Corti, M. Cobanaj, E.C. Dee [et al.] // Cancer Treatment Reviews. — 2022. — № 112. — P. 102498.

3. Mullachery B. A Smart Healthcare Framework: Opportunities for Integrating Emerging Technologies (5G, IoT, AI, and GIS) / B. Mullachery, S. Alismail // Proceedings of the Future Technologies Conference. — 2022. — Vol. 3. — P. 325–340.

4. Padhy N.P. Artificial Intelligence and Intelligent Systems / N.P. Padhy. — Oxford : Oxford Univ. Press, 2005. — 632 p.

5. Gupta M. Explainable Artificial Intelligence (XAI): Understanding and Future Perspectives / M. Gupta // Studies in Computational Intelligence. — 2023. — Vol. 1072. — P. 19–33.

6. The Role of AI and Automation on the Future of Jobs and the Opportunity to Change Society / M. Au-Yong-Oliveira, D. Canastro, J. Oliveira [et al.] // New Knowledge in Information Systems and Technologies : World Conference on Information Systems and Technologies, 30 March, 2019. — Cham : Springer, 2019. — P. 348–357.

7. Прохоренко Ю.И. Безусловный базовый доход: практика и историческая перспектива / Ю.И. Прохоренко, З.А. Красномовец. — EDN ALTURV // Ученые заметки ТОГУ. — 2019. — Т. 10, № 1. — С. 222–233.

8. Козлов А.В. Гарантированный базовый доход: экономическое и этическое измерения / А.В. Козлов. — EDN KPUTQQ // Научные труды Республиканского института высшей школы. — 2019. — № 18. — С. 374–381.

9. Садовая Е.С. Концепция и реализация идеи безусловного базового дохода в контексте трансформации социально-трудовой сферы / Е.С. Садовая. — DOI 10.34022/2658-3712-2020-38-1-59-72. — EDN SRSOOJ // Социально-трудовые исследования. — 2020. — № 1. — С. 59–72.

10. Kukkala V.K. Roadmap for Cybersecurity in Autonomous Vehicles / V.K. Kukkala, S.V. Thiruloga, S. Pasricha // IEEE Consumer Electronics Magazine. — 2022. — № 11. — P. 13–23.

11. Madani M. The Role of Deep Learning in Advancing Breast Cancer Detection Using Different Imaging Modalities: A Systematic Review / M. Madani, M.M. Behzadi, S. Nabavi // Cancers. — 2022. — № 14. — P. 5334.

12. Artificial Intelligence Predicts Lymph Node Metastasis or Risk of Lymph Node Metastasis in T1 Colorectal Cancer / K. Kasahara, K. Katsumata, A. Saito [et al.] // International Journal of Clinical Oncology. — 2022. — № 27. — P. 1570–1579.

13. Xu Z. The possibilities and limits of AI in Chinese Judicial Judgment / Z. Xu, Y. Zhao, Z. Deng // AI and Society. — 2022. — № 37. — P. 1601–1611.

14. Rotaru V. Event-level Prediction of Urban Crime Reveals a Signature of Enforcement Bias in US Cities / V. Rotaru, Y. Huang, T. Li // Nature Human Behavior. — 2022. — № 6. — P. 1056–1068.

15. Assessing Bank Default Determinants via Machine Learning / V. Lagasio, F. Pampurini, A. Pezzola, A.G. Quaranta // Information Sciences. — 2022. — № 618. — P. 87–97.

16. Решетников А.Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) / А.Ю. Решетников, Е.А. Русскевич // Законы России: опыт, анализ, практика. — 2018. — № 2. — С. 51–55.

17. Adversarial Attacks and Defenses in Images, Graphs and Text: A Review / X. Han, M. Yao, L. Hao-Chen [et al.] // International Journal of Automation and Computing. — 2020. — № 1. — P. 151–178.

18. Dremliuga R. How Development of Artificial Intelligence Technology will Cause Changes in Crime and Criminal Law / R. Dremliuga // AI for Everyone: benefitting from and building trust in the technology / ed. T. Walsh, 2020. — P. 24–25.

19. Shoplifting Smart Stores using Adversarial Machine Learning / M. Nassar, A. Itani, M. Karout [et al.] // 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, 2019. — P. 1–6.

20. Паркин А.Н. Состязательные атаки на нейронную сеть распознавания лиц / А.Н. Паркин. — EDN EPCNCE // Ломоносов-2019 : сб. тезисов XXVI Междунар. науч. конф., Москва, 8 апр. 2019 г. — Москва, 2019. — С. 152–153.

21. Gan H. An Autoencoder Based Approach to Defend against Adversarial Attacks for Autonomous Vehicles / H. Gan, C. Liu. — DOI 10.1109/MetroCAD48866.2020.00015 // 2020 International Conference on Connected and Autonomous Driving (MetroCAD). — 2020. — P. 43.

22. Беспилотники на дорогах России (уголовно-правовые проблемы) / А.И. Воробьев, С.В. Жанказиев, С.А. Иванов [и др.]. — Москва : Проспект, 2021. — 520 с. — EDN TCUOLW.

23. End-to-end Attack on Text-based CAPTCHAs Based on Cycle-Consistent Generative Adversarial Network / C. Li, X. Chen, H. Wang [et al.] // Neurocomputing. — 2021. — № 433. — P. 223–236.

24. Chen D. Cyber Security in Smart Cities: A Review of Deep Learning-Based Applications and Case Studies / D. Chen, P. Wawrzynski, Z. Lv. — DOI org/10.1016/j.scs.2020.102655 // Sustainable Cities and Society. — 2021. — № 66.

25. Шваб К. Технологии Четвертой промышленной революции / К. Шваб. — Москва : Эксмо, 2018. — 320 с.

26. Brundage M. The Malicious use of Artificial intelligence: Forecasting, Prevention, and Mitigation / M. Brundage, S. Avin., J. Clark [et al.]. — 2018. — DOI org/10.48550/arXiv.1802.07228. — URL: https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf.

27. Pavlitskaya S. Feasibility and Suppression of Adversarial Patch Attacks on End-to-End Vehicle Control / S. Pavlitskaya, S. Ünver, J.M. Zöllner. — DOI 10.1109/ITSC45102.2020.9294426 // 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC). — 2020. — URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9294426.

28. Mingtsung C. Research on the Application of Artificial Intelligence Technology in the Field of Justice / C. Mingtsung, L. Shuling. — DOI 10.1088/1742-6596/1570/1/012047 // Journal of Physics: Conference Series. — 2020. — № 1570.

29. Road Traffic Prediction Model Using Extreme Learning Machine: The Case Study of Tangier, Morocco / M. Jiber, A. Mbarek., A. Yahyaouy [et al.]. — DOI 10.3390/info11120542 // Information (Switzerland). — 2020. — № 11. — P. 1–15.

REFERENCES

1. Günsberg P.S. Automated Vehicles — is a Dilution of Human Responsibility the Answer? *New Journal of European Criminal Law*, 2022, no. 13, pp. 439–451.

2. Corti C., Cobanaj M., Dee E.C., Celi L.A., Curigliano G. Artificial Intelligence in Cancer Research and Precision Medicine: Applications, Limitations and Priorities to Drive Transformation in the Delivery of Equitable and Unbiased Care. *Cancer Treatment Reviews*, 2022, no. 112, pp. 102498.

3. Mullachery B., Alismail S. A Smart Healthcare Framework: Opportunities for Integrating Emerging Technologies (5G, IoT, AI, and GIS). *Proceedings of the Future Technologies Conference*, 2022, vol. 3, pp. 325–340.

4. Padhy N.P. *Artificial Intelligence and Intelligent Systems*. Oxford University Press, 2005. 632 p.

5. Gupta M. Explainable Artificial Intelligence (XAI): Understanding and Future Perspectives. *Studies in Computational Intelligence*, 2023, vol. 1072, pp. 19–33.

6. Au-Yong-Oliveira M., Canastro D., Oliveira J., Tomás J., Amorim S., Moreira F. The Role of AI and Automation on the Future of Jobs and the Opportunity to Change Society. *New Knowledge in Information Systems and Technologies : World Conference on Information Systems and Technologies, 30 March, 2019*, Cham, Springer, 2019, pp. 348–357.

7. Prokhorenko Yu.I., Krasnomovets Z.A. Bedingungsloses Grundeinkommen:Praxis und Historische Perspektive. *Uchenye zametki TOGU = Scientists' Notes PN*, 2019, vol. 10, no. 1, pp. 222–233. (In Russian). EDN: ALTURV.

8. Kozlov A.V. Guaranteed Basic Income: Economic and Moral Dimension. *Nauchnye trudy Respublikanskogo instituta vysshei shkoly = Scientific Works of the Republican Institute of Higher Education*, 2019, no. 18, pp. 374–381. (In Russian). EDN: KPUTQQ.

9. Sadovaya E.S. Concept and Implementation of the Idea of Universal Basic Income in the Context of Changing Social Labor Sphere. *Sotsial'no-trudovye issledovaniya = Social & Labor Research*, 2020, no. 1, pp. 59–72. (In Russian). EDN: SRSOOJ. DOI: 10.34022/2658-3712-2020-38-1-59-72.

10. Kukkala V.K., Thiruloga S.V., Pasricha S. Roadmap for Cybersecurity in Autonomous Vehicles. *IEEE Consumer Electronics Magazine*, 2022, no. 11, pp. 13–23.

11. Madani M., Behzadi M.M., Nabavi S. The Role of Deep Learning in Advancing Breast Cancer Detection Using Different Imaging Modalities: A Systematic Review. *Cancers*, 2022, no. 14, pp. 5334.

12. Kasahara K., Katsumata K., Saito A., Kuroda M., Tsuchida A. Artificial Intelligence Predicts Lymph Node Metastasis or Risk of Lymph Node Metastasis in T1 Colorectal Cancer. *International Journal of Clinical Oncology*, 2022, no. 27, pp. 1570–1579.

13. Xu Z., Zhao Y., Deng Z. The Possibilities and Limits of AI in Chinese Judicial Judgment. *AI and Society*, 2022, no. 37, pp. 1601–1611.

14. Rotaru V., Huang Y., Li T. Event-level Prediction of Urban Crime Reveals a Signature of Enforcement Bias in US Cities. *Nature Human Behavior*, 2022, no. 6, pp. 1056–1068.

15. Lagasio V., Pampurini F., Pezzola A., Quaranta A.G. Assessing Bank Default Determinants via Machine Learning. *Information Sciences*, 2022, no. 618, pp. 87–97.

16. Reshetnikov A.Yu., Russkevich E.A. On Criminal Liability for Unlawful Influence on the Critical Information Infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of Russia). *Zakony Rossii: opyt, analiz, praktika = Law of Russia: Experience, Analysis, Practice*, 2018, no. 2, pp. 51–55. (In Russian).

17. Han X., Yao M., Hao-Chen L., Debayan D., Hui L., Ji-Liang T., Anil K. Adversarial Attacks and Defenses in Images, Graphs and Text: A Review. *International Journal of Automation and Computing*, 2020, no. 17, pp. 151–178.

18. Dremliuga R. How Development of Artificial Intelligence Technology will Cause Changes in Crime and Criminal Law. In Walsh T. (ed.). *AI for Everyone: benefitting from and building trust in the technology*, 2020, pp. 24–25.

19. Nassar M., Itani A., Karout M., El Baba M., Kaakaji O.A.S. Shoplifting Smart Stores Using Adversarial Machine Learning. *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*. Abu Dhabi, 2019, pp. 1–6.

20. Parkin A.N. Adversarial Attacks Against the Neural Face Recognition Network. *Lomonosov-2019, Collection of Abstracts of the XXI International Scientific Conference, Moscow, April 8, 2019.* Moscow, 2019, pp. 152–153. (In Russian). EDN: EPCNCE.

21. Gan H., Liu C. Autoencoder Based Approach to Defend against Adversarial Attacks for Autonomous Vehicles. *2020 International Conference on Connected and Autonomous Driving (MetroCAD)*, 2020, pp. 43. DOI: 10.1109/MetroCAD48866.2020.00015.

22. Vorob'ev A.I., Zhankaziev S.V., Ivanov S.A., Korobeev A.I., Malikov S.V. *Unmanned Vehicles on Russian Roads (Criminal Law Problems)*. Moscow, Prospekt Publ., 2021. 520 p. EDN: TCUOLW.

23. Li C., Chen X., Wang H., Zhang Y., Wang W. End-to-End Attack on Text-based CAPTCHAs Based on Cycle-Consistent Generative Adversarial Network. *Neurocomputing*, 2021, no. 433, pp. 223–236.

24. Chen D., Wawrzynski P., Lv Z. Cyber Security in Smart Cities: A Review of Deep Learning-Based Applications and Case Studies. *Sustainable Cities and Society*, 2021, no. 66. DOI: org/10.1016/j.scs.2020.102655.

25. Schwab K. *The Fourth Industrial Revolution.* Geneva, 2016. 184 p. (Russ. ed.: Schwab K. *The Fourth Industrial Revolution*. Moscow, Eksmo Publ., 2018. 320 p.).

26. Brundage M., Avin S., Clark J., Toner H., Eckersley P. *The Malicious USE of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. 2018. DOI: org/10.48550/arXiv.1802.07228. URL: https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf.

27. Pavlitskaya S., Ünver S., Zöllner J.M. Feasibility and Suppression of Adversarial Patch Attacks on End-to-End Vehicle Control. *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC),* 2020. DOI: 10.1109/ITSC45102.2020.9294426. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9294426.

28. Mingtsung C., Shuling L. Research on the Application of Artificial Intelligence Technology in the Field of Justice. *Journal of Physics: Conference Series*, 2020, no. 1570. DOI 10.1088/1742-6596/1570/1/012047.

29. Jiber M., Mbarek A., Yahyaouy A., Sabri M.A., Boumhidi J. Road Traffic Prediction Model Using Extreme Learning Machine: The Case Study of Tangier, Morocco. *Information (Switzerland)*, 2020, no. 11, pp. 1–15. DOI: 10.3390/info11120542.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Дремлюга Роман Игоревич — доцент Юридической школы Дальневосточного федерального университета, кандидат юридических наук, г. Владивосток, Российская Федерация; e-mail: dremliuga.ri@dvfu.ru.

Коробеев Александр Иванович — заведующий кафедрой уголовного права и криминологии Дальневосточного федерального университета, доктор юридических наук, профессор, заслуженный деятель науки Российской Федерации, г. Владивосток, Российская Федерация; e-mail: akorobeev@rambler.ru.

ДЛЯ ЦИТИРОВАНИЯ

Дремлюга Р.И. Преступные посягательства на системы искусственного интеллекта: уголовно-правовая характеристика / Р.И. Дремлюга, А.И. Коробеев. — DOI 10.17150/2500-1442.2023.17(1).5-12. — EDN USOFCJ // Всероссийский криминологический журнал. — 2023. — Т. 17, № 1. — С. 5–12.

INFORMATION ABOUT THE AUTHORS

Dremliuga, Roman I. — Ass. Professor, Law School, Far Eastern Federal University, Ph.D. in Law, Vladivostok, the Russian Federation; e-mail: dremliuga.ri@dvfu.ru.

Korobeev, Alexander I.— Head, Chair of Criminal Law and Criminology, Far Eastern Federal University, Doctor of Law, Professor, Honored Researcher of the Russian Federation, Vladivostok, the Russian Federation; e-mail: akorobeev@rambler.ru.

FOR CITATION

Dremliuga R.I., Korobeev A.I. Criminal Infringement on Artificial Intelligence Systems: a Criminal Law Description. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 1, pp. 5–12. (In Russian). EDN: USOFCJ. DOI: 10.17150/2500-1442.2023.17(1).5-12.