DOI: 10.17803/1729-5920.2021.173.4.063-070

М. А. Желудков*

Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды

Аннотация. Недооценка важности решения проблем в деятельности правоохранительных органов в контексте применения преступниками новых цифровых технологий может привести к тому, что высокотехнологичная преступность не заменит, например, традиционные формы хищений, но может придать эффект резкой гипоксии предупредительной деятельности, при которой не хватит запланированных правоохранительных сил и средств реагирования на возникающие угрозы. Актуальность статьи заключается в том, что при оценке использования современных цифровых технологий в научной литературе и нормативном обеспечении особый упор делается на специфические функции данных технологий автоматически анализировать какой-либо массив данных и с помощью набора алгоритмов принимать решения по оптимизации процессов и деятельности, то есть способности упростить человеческие взаимоотношения. Однако опыт правоохранительной деятельности показывает, что отсутствие правоохранительного обеспечения защиты общества от негативного использования технологий приводит к тому, что реакция следует уже на преступные последствия их применения. Создание систем искусственного интеллекта (ИИ) привело к серьезным социальным изменениям, происходит своеобразная трансформация общественных отношений под влиянием цифровой экономики, которая неизбежно создает предпосылки для зарождения особого преступного поведения. В статье был сделан краткий анализ информации из открытых источников о возможностях преступного применения искусственного интеллекта. Поставлена цель проанализировать различные возможности создания новой модели защиты от киберпреступности под контролем правоохранительных органов в условиях новых угроз от преступного использования технологий ИИ и новой промышленной революции.
Ключевые слова: искусственный интеллект; кибербезопасность; цифровые технологии; киберпреступность; дипфейк; защита от киберпреступности; модель защиты; цифровая экономика; персональные данные.
Для цитирования: *Желудков М. А.* Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // Lex russica. — 2021. — Т. 74. — № 4. — С. 63–70. — DOI: 10.17803/1729-5920.2021.173.4.063-070.

Justification of the Necessity to Adjust Law Enforcement Agencies to Digital Transformation of Criminality

Mikhail A. Zheludkov, Dr. Sci. (Law), Associate Professor, Professor of the Department of Criminal Law and Applied Informatics in Jurisprudence, Law Institute, Tambov State Technical University
ul. Internatsionalnaya, d. 33, Tambov, Russia, 392000
kandydat1@yandex.ru

Abstract. Underestimation of the importance of solving problems in law enforcement agencies in the context of the use of new digital technologies by criminals may lead to the situation when high-tech crime does not

* *Желудков Михаил Александрович,* доктор юридических наук, доцент, профессор кафедры уголовного права и прикладной информатики в юриспруденции Юридического института Тамбовского государственного технического университета
Интернациональная ул., д. 33, г. Тамбов, Россия, 392000
kandydat1@yandex.ru

replace traditional forms of theft, but may result in a sharp hypoxia of preventive activities, which will lack the planned law enforcement resources and means of responding to emerging threats. The relevance of the paper lies in the fact that when assessing the use of modern digital technologies in scientific literature and regulatory support, special emphasis is placed on specific data functions of technologies to automatically analyze a set of data and with the help of a set of algorithms to make decisions on optimization of processes and activities, that is, the ability to simplify human relationships. However, the experience of law enforcement has shown that the lack of law enforcement support for protecting the society from negative use of technology leads to the fact that the response now follows the criminal consequences of their use of technologies. The creation of artificial intelligence (AI) systems has led to serious social changes, there is a kind of transformation of public relations under the influence of the digital economy, which inevitably creates the prerequisites for the emergence of specific criminal behavior. The paper provides for a brief analysis of information from open sources about the possibilities of criminal use of artificial intelligence. The author aims to analyze the various possibilities of creating a new model of protection against cybercrime under the control of law enforcement agencies in the context of new threats caused by criminal use of AI technology and the new industrial revolution.
Keywords: artificial intelligence; cybersecurity; digital technology; cybercrime; deepfake; protection against cybercrime; protection model; digital economy; personal data.
Cite as: Zheludkov MA.Obosnovanie neobkhodimosti adaptatsii deyatelnosti pravookhranitelnykh organov k usloviyam tsifrovoy transformatsii prestupnoy sredy [Justification of the Necessity to Adjust Law Enforcement Agencies to Digital Transformation of Criminality] *Lex russica*. 2021;74(4):63-70. DOI: 10.17803/1729-5920.2021.173.4.063-070. (In Russ., abstract in Eng.).

В последние годы наряду с терминами «профилактика», «предупреждение» и «борьба с традиционной преступностью» в литературе, средствах массовой информации, а также положениях нормативных документов в повседневный обиход работы правоохранительных органов входят термины правоохранительной защиты от преступности в цифровом информационном пространстве. Применение новых цифровых технологий ставит целью достижение экономического развития, повышение научного потенциала общества, создание предпосылок для формирования комфортной и безопасной окружающей среды для конкретного человека.

Однако повсеместное внедрение интернет-торговли, использование цифровых средств видеонаблюдения, технологий робототехники и искусственного интеллекта не только позволяет развивать возможности цифровой экономики, но и создает предпосылки к появлению таких негативных последствий, как цифровая трансформация традиционной преступности при отсутствии системы правоохранительной защиты от данной опасности. Из данных Генеральной прокуратуры РФ следует, что уровень киберпреступности к 2019 г. вырос на 70 % по сравнению с 2018 г. и на 150 % по сравнению с 2013 г. (180 153 преступления — 66 000 преступлений)[1]. С одной стороны, подобное увеличение свидетельствует об усилении борьбы с данным явлением, с другой стороны, видим серьезное запаздывание реакции всей системы профилактического воздействия на резкое увеличение уровня киберпреступности. Недооценка важности решения проблем в деятельности правоохранительных органов в контексте применения преступниками новых цифровых технологий может привести к тому, что высокотехнологичная преступность не заменит, например, традиционные формы хищений, но может придать эффект резкой гипоксии предупредительной деятельности, при которой не хватит запланированных правоохранительных сил и средств реагирования на возникающие угрозы. При оценке использования современных цифровых технологий в научной литературе и нормативном обеспечении особый упор делается на специфические функции данных технологий автоматически анализировать какой-либо массив данных и с помощью набора алгоритмов принимать решения по оптимизации процессов и деятельности, то есть на способности упростить человеческие взаимоотношения. Однако опыт правоохранительной деятельности показывает, что отсутствие правоохранительного обеспечения защиты общества от негативного использования технологий приводит к тому, что реакция следует уже на преступные последствия их применения. Большая часть данной преступности совершается с использованием

[1] Киберпреступность в России растет быстрее любых других видов преступлений // URL: https://safe.cnews.ru/news/top/2019-09-27_kiberprestupnost_v_rossii (дата обращения: 21.10.2020).

сети «Интернет» и новых технологий перевода денежных средств. Около 70 % данных преступлений совершается в группах, где хотя бы один из преступников обладает узкой специализацией в области компьютерной информации или компьютерных технологий. Таким образом, можно сделать обоснованный вывод о том, что новые цифровые технологии в определенной криминальной ситуации могут стать средством совершения мошеннических действий или других форм преступных действий. Поэтому, если на данный момент существуют определенные сложности с запретом применения новых технологических решений, так как их применение — это объективный процесс развития общества, то нужно задать себе вопрос о том, каким образом эти технологии могут быть использованы при совершении преступлений и как правоохранительным органам системно защищать общество в этих новых условиях промышленной революции?

В контексте подобного анализа обратим внимание на программы искусственного интеллекта (ИИ). Технология ИИ основана на алгоритмах автоматического взаимодействия компьютерной системы и реакций окружающего мира, где с помощью нейронных сетей происходит автоматическая имитация определенной умственной функции человеческого бытия. В бытовом смысле с программами искусственного интеллекта общество сталкивается постоянно по мере автоматизации каких-либо сфер человеческой деятельности. Например, поисковая система в интернет-пространстве, лифтовое оборудование в многоквартирном доме, система безналичной оплаты банковскими картами, прокладка маршрута на карте, распознавание образов и отпечатков пальцев рук в смартфонах, алгоритм T9 при наборе текста и др. Причем подобное использование указанных программ уже становится будничным занятием, но, используя их положительные стороны, нельзя не анализировать и те угрозы, которые они несут при негативном использовании. Например, антивирусная программа — необходимый компонент любого компьютера и сложный искусственный интеллект, но отдельный вирус, а их пишутся миллионы, может стать той программой, которая не будет им распознана и, соответственно, появляется возможность использования системы искусственного интеллекта для совершения корыстного преступления или получения, распространения определенной информации.

Поэтому при создании своевременных мер защиты от киберпреступности в обязательном порядке следует учитывать специфическую сторону данных преступлений, а именно то, что преступность в сфере цифровой экономики — новое, сложное социальное явление, где негативные экономико-социальные процессы не являются непосредственной причиной общественно опасных деяний, а промышленная революция способна порождать массовость определенного преступного поведения. Соглашаясь с тем, что создание системы ИИ приводит к серьезным социальным изменениям, считаем, что своеобразная трансформация общественных отношений под влиянием цифровой экономики неизбежно создает предпосылки для зарождения особого преступного поведения. Многие преступления в киберпространстве ранее нельзя было совершить без появления новых технологических способов и программ. Анализ развития киберпреступности свидетельствует о том, что она является своеобразной реакцией определенных потенциальных преступников на цифровую трансформацию общественных отношений. Ключевым моментом в данном сочетании является то, что новые цифровые технологии способны как последовательно развивать различные сферы человеческой деятельности, так и создавать новые криминальные возможности, способы и средства совершения преступлений. Современные программы искусственного интеллекта позволяют не только собирать персональные данные по каждой личности, но и создавать так называемые психофизиологические профили лица. В этих профилях собирается информация о семье, детях, предпочтениях и хобби, посещаемых местах и заказах. Подобные сведения позволяют выстроить механизм воздействия на личность, создавая, например, новые способы кибермошенничества.

В качестве примера использования программ ИИ при совершении преступлений приведем сведения Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (ФинЦЕРТ). Данная организация выявила «новый способ хищения средств со счетов клиентов в банке с использованием Системы быстрых платежей (СБП). При установке в мобильном банке одной из кредитных организаций возможности переводов по СБП была оставлена уязвимость, связанная с открытым API-интерфейсом. Через нее мошенники смогли подменять счета отпра-

вителя. Злоумышленник через уязвимость в одной из банковских систем получил данные счетов клиентов. Затем он запустил мобильное приложение в режиме отладки, авторизовавшись как реальный клиент, отправил запрос на перевод средств в другой банк, но перед совершением перевода вместо своего счета отправителя средств указал номер счета другого клиента этого банка. ДБО, не проверив, принадлежит ли указанный счет отправителю, направило в СБП команду на перевод средств, который она и осуществила. Так мошенники отправляли себе деньги с чужих счетов. Номера счетов жертв были получены в ходе успешной атаки по использованию недокументированной возможности API (программного интерфейса приложения) дистанционного банковского обслуживания (ДБО)»[2].

Подобный и другие примеры использования программ ИИ при совершении преступлений прямо указывают на то, что, разрабатывая меры защиты от киберпреступности со стороны правоохранительных органов, необходимо своевременно проводить анализ новых цифровых технологий на предмет получения качественной и полноценной информации о потенциальной возможности использования этих продуктов преступниками при совершении преступлений.

Например, необходимо сразу обозначить приоритеты: не программы искусственного интеллекта создают угрозы, социальные проблемы и киберпреступность. Искусственный интеллект на данном этапе развития общества сам по себе не крадет информацию, не увольняет людей, заменяя их рабочую функцию, не снимает деньги с банковских карт. Криминальные угрозы не возникают в результате создания новых технологий или устройств. Эти технологии можно назвать лишь средством удовлетворения антисоциальных потребностей со стороны потенциальных преступников. Если в нашей стране отсутствует системное обеспечение защиты прав и законных интересов человека и общества от негативного воздействия программ ИИ, то нельзя говорить только о недостатках этих программ.

На государственном уровне подобными вопросами реализации новых технологий и защиты от них общества занимаются постоянно. В частности, «в рамках реализации Указа Президента Российской Федерации от 7 мая 2018 г. № 204 “О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года” происходит обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере, сформирована национальная программа “Цифровая экономика Российской Федерации”»[3].

Однако в представленных и других документах по развитию цифровых технологий мы так и не находим отражения элементов деятельности и взаимодействия правоохранительных и иных органов по вопросам профилактической защиты личности, общества и государства от негативных элементов внедрения новых цифровых инструментов. Попробуем обосновать данный посыл на примере появления и использования в сети Интернет новых программ искусственного интеллекта, основанных на методе подмены лица — дипфейк. Дипфейк (Deepfake, от Deep learning — глубинное обучение и Fake — подделка) является синтезом изображения, основанным на искусственном интеллекте. Программа соединяет и накладывает существующие изображения и видео на исходный фото- или видеообъект нейросети (GAN). Одна часть алгоритма учится на реальных фотографиях определенного объекта и создает изображение, буквально «состязаясь» со второй частью алгоритма, пока та не начнет путать копию с оригиналом[4].

Представленная технология изменения изображений лица на фото- и видеоматериалах создает для потенциальных преступников реальные возможности для совершения различных мошеннических действий. Например, подобные технологии в условиях удаленного доступа могут быть использованы для оформления под-

---

[2] *Буйлов М.* Система хитрых платежей // URL: https://www.kommersant.ru/doc/4465889 (дата обращения: 14.08.2020).

[3] Национальная программа «Цифровая экономика Российской Федерации» // URL: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 14.08.2020).

[4] Deepfake // URL: https://ru.wikipedia.org/wiki/Deepfake#mw-head (дата обращения: 14.08.2020) ; *Brandon J.* Terrifying high-tech porn: Creepy ‘deepfake’ videos are on the rise // Fox News. 16 February 2018. URL: https://ru.wikipedia.org/wiki/Deepfake#mw-head (дата обращения: 14.08.2020) ; *Созанкова Е.* Дипфейки: как нейросети копируют реальность // URL: https://ru.wikipedia.org/wiki/Deepfake#mw-head (дата обращения: 14.08.2020).

ложных товарно-денежных операций, получении обманом кредитных ресурсов, изменения доказательств по реальным уголовным делам. Если сегодня такие программы пока еще недостаточно совершенны, то пройдет небольшой промежуток времени, и технология дипфейков с открытым кодом создаст серьезные трудности в идентификации аудио- и видеоинформации в интернет-пространстве. Для копирования голоса человека будет достаточно 20–30 минут его разговора в записи. В этом случае увеличится количество мошеннических действий, где от имени руководства или собственников предприятий будут поступать указания на перевод денежных средств или продажу активов, проведение по телефону банковских операций и др.

Кроме подобных технологий, обратим внимание и на то, каким образом сегодня используются данные видеоконтроля общественной безопасности на определенной территории. В данной ситуации программы ИИ не только дают возможность записывать и хранить информацию с видеокамер, но и позволяют создавать системные возможности по тотальному цифровому контролю граждан в общественных местах. Например, в Китае видеоконтроль встроен в систему государственного кредита, где каждый гражданин получает своеобразный социальный балльный рейтинг. В основе получения баллов лежит его общественная жизнь и персональная информация. От рейтинга зависит получение определенных разрешений на сферы деятельности, получение кредитов и др. Подобные системы в разной интерпретации действуют и в других странах мира.

В России одним из первопроходцев в данном направлении является Правительство г. Москвы. В частности в 2020 г. «Департамент информационных технологий Москвы разместил тендер о разработке системы, непрерывно отслеживающей активность жителей на территории Москвы и в городских объектах. В рамках "информационной системы мониторинга и анализа интернет-активности" (ИС СТАТС) предлагается создать подробные профили пользователей всех городских услуг. Профили среди прочего будут содержать сведения об оплате услуг, задолженностях, штрафах, например, за нарушение ПДД и правил парковки, данные о проездном документе и социальной карте. Система СТАТС будет сопоставлять эту информацию с данными, полученными из общественных точек доступа к вай-фаю и от операторов связи. Также она станет отслеживать территориальные запреты, "медицинские ограничения" и "лояльность" пользователя»[5]. Пока сбор этих данный предусматривается в обезличенном виде от персональных сведений. Не забываем и о том, что с 2012 г. в г. Москве действует система «Умный город», которая позволяет отслеживать передвижения граждан посредством соотнесения данных с видеокамер, точек вай-фая, сотовых систем и т.д.

Создание подобных и других систем имеет как подвижников новых решений, так и противников, которые полагают, что в обществе могут быть созданы условия для тоталитарного цифрового режима. Не вступая в дискуссию по данному вопросу, тем не менее отметим, что положительной составляющей данных проектов всегда является снижение уровня насильственной и корыстной преступности в общественных местах. Но вновь обозначим момент того, что не сами новые программы ИИ совершают преступление. Мотивы человеческого поведения всегда будут иметь корыстную или иную мотивационную направленность, в том числе запретную. Именно поэтому безопасность личности, общества и государства в этом вопросе должна представлять собой не отдельную функцию, а системный качественный процесс по применению технологий защиты от незаконного использования данных цифровых решений. Система защиты состоит из множества элементов, каждый из которых составляет своеобразную подсистему. В нашем случае подразумевается создание системы защиты личности, общества и государства от киберпреступности на основе и с учетом технологий ИИ. Защита — это деятельность по обеспечению безопасности определенного объекта.

Раздробленность действий правоохранительных органов в этом вопросе не может привести к однозначно высокому результату их работы. Оценка сведений по готовности системы правоохранительного реагирования на применение преступниками программ искусственного интеллекта приводит нас к неутешительному выводу о том, что на данном временно́м отрезке уровень профессиональных компетен-

[5] *Бакланов А.* Мэрия Москвы заказала непрерывный мониторинг активности горожан // URL: https://meduza.io/feature/2020/11/24/meriya-moskvy-zakazala-nepreryvnyy-monitoring-aktivnosti-gorozhan-vlasti-budut-sledit-za-dolgami-shtrafami-i-meditsinskimi-ogranicheniyami (дата обращения: 25.11.2020).

ций в этой области не в соответствующей мере развит с точки зрения совершаемых киберпреступлений. Каждый правоохранительный орган, в зависимости от юрисдикционной и территориальной подследственности, концентрирует свои усилия по отдельным видам компьютерных преступлений. Изучая деятельность различных правоохранительных органов, мы не выявили их возможности по системной цифровой защите и контролю над криминальной интернет-средой. При решении повседневных задач правоохранительная система реагирует только на уже возникшие опасности, на зарегистрированные преступления. Каждый правоохранительный орган занимается мониторингом информационного интернет-окружения в зависимости от поставленных руководством задач и подследственности совершенных деяний. Частично это происходит от недооценки реальности перерастания отдельных угроз от незаконного использования программ ИИ в угрозу национальной безопасности России. Действительно, несмотря на широкое использование терминологии и программ искусственного интеллекта, на практике и в теории более склонны развиваться мысли о том, как применить данные технологии в социальной, экономической или другой сфере жизнедеятельности людей. Опросы экспертов, сотрудников органов внутренних дел, непосредственно занимающихся борьбой с преступностью, показали, что более 85 % сотрудников уголовного розыска и следствия имеют поверхностные знания по этой проблематике. Их подход к этой проблеме зиждется на том, что ИИ не может сегодня самостоятельно решать человеческие задачи, а технологический потенциал правоохранительных органов позволяет установить местонахождение преступника. Однако подобный подход не отвечает на вопрос о том, что мы будем делать при таком развитии программирования, когда имитационные возможности ИИ с помощью алгоритмов и программ нивелируют эти возможности, и отличить цифровую машину от человека будет возможно только с помощью этой же цифровой технологии?

Как мы уже отмечали ранее, значительное и всё возрастающее количество информационных данных по использованию ИИ при совершении различного рода преступлений, программы которого становятся всё более доступными, фактически уже является доказательством необходимости перехода к более эффективной организации обеспечения защиты от киберпреступности. Функционал подобной системы не должен замыкаться на какой-либо существующий правоохранительный орган и связанные с ним проблемы правоохранительного реагирования. Назрела насущная потребность в создании нового, более технически и организационно оснащенного правоохранительного органа для эффективного отражения кибератак и защиты от высокотехнологической преступности во всех сферах жизнедеятельности нашего общества. Структурная составляющая данного органа может иметь разное наполнение, но она должна быть построена на возможности получения информации по всем программам ИИ и киберпреступлениям, а также должна иметь возможности по защите объектов от вирусных атак на территории России. Необходимо видеть общую картину киберпреступности, анализировать способы совершения преступлений с использованием программ ИИ, а также иметь более ранние возможности по установлению местонахождения киберпреступников и своевременному блокированию их технологических программ.

Поскольку для изучения деятельности правоохранительных органов в литературе и нормативных документах применяется различная терминология воздействия на преступность и можно ожидать того, что будет трудно добиться соответствующего конкретизированного терминологического определения в этой области, всё же предполагаем, что для данного правоохранительного органа более приемлемо обозначить именно защитные функции. Защита от киберпреступности предполагает, что данный орган не должен заниматься борьбой или расследованием этих преступлений, на это есть сотрудники других органов. Нет, в его задачи должны быть внесены мероприятия по технологическим, аналитическим и функционально детерминирующим элементам системы защиты, где каждая мера будет направлена на создание вокруг киберпространства своеобразного барьера недопустимых действий, преодоление которого и будет считаться преступным. Важно своевременно выявлять структурные компоненты цифровой среды, применяемые для совершения киберпреступлений: социальные сети, хакеров, сетевые группы по интересам и др. Для большей эффективности мер защиты следует задуматься о переводе в цифровой режим всех форм статистических карточек, обвинительных заключений, приговоров для их последующего анализа на основе алгоритма нейросетей ИИ и выделения опре-

деленной категории личности преступника, способного совершать определенные деяния.

Особо следует обозначить баланс защиты от киберпреступности и частной жизни граждан. Вопросы применения ИИ обязательно влекут за собой проблемы конфиденциальной защиты персональных данных простого человека. Исходя из правил русского языка в содержание понятия «конфиденциальные» закладываются элементы тайны, то есть ограничения доступа к личным сведениям и отсутствия огласки этих сведений без согласия лица. Персонализация представляет собой любую информацию о человеке, которая позволяет его выделить, идентифицировать среди других людей. В отношении защиты подобных данных обратим внимание на международный опыт. Например, в Китае одним из способов защиты является полный контроль государства за действием личности в сети Интернет. «При регистрации в социальных сетях и на других сайтах пользователь обязан вводить паспортные данные. Такие меры были вызваны распространением клеветы, недобросовестной рекламы и мошенничества в киберпространстве КНР»[6].

С учетом в том числе и зарубежного опыта предлагаем при проведении мероприятий защиты предоставить указанному правоохранительному органу полномочия по проверке персональной ответственности конкретных лиц за контроль принятия в автоматическом режиме системой ИИ решений, направленных на изменение прав и интересов конкретного человека. В данной ситуации важно понимание того, каким образом должны храниться цифровые данные о личности, каковы нормативные возможности банков и иных органов продавать или передавать другим лицам персональную идентификационную информацию, как решение ИИ может быть проверено и завизировано подписью конкретного лица? В противном случае, например, мошенничество при приеме в вузы с помощью необоснованного приоритета и отказа будет списано на действие машинного комплекса и не будет иметь профилактического и уголовно-правового уровня защиты личности.

С учетом создания единого центра защиты от киберпреступлений следует предусмотреть те элементы кибербезопасности, которые сегодня будут адекватны новой промышленной революции. В процессе создания новой социальной интернет-реальности не должно быть обезличенных контактов. Поэтому при входе и использовании информационных интернет-ресурсов должна быть выделена контрольная функция человека. Вновь обозначим необходимость использования паспортных данных для входа на социальные платформы и сайты. Подобная мера защиты позволит своевременно установить и заблокировать IP-адрес компьютера, с которого совершается финансовое мошенничество, вирусная атака или незаконное использование персональных данных. Подобные способы защиты общества от киберпреступности являются и своеобразной защитой персональных данных, так как их последующее использование операторами интернет-ресурсов будет контролироваться соответствующим государственным органом.

Таким образом, в статье выдвигается тезис о том, что главной теоретической проблемой при создании новой модели защиты от киберпреступности является недостаточность понимания на государственном уровне того, что разработка и внедрение программ ИИ в России должны реализовываться под контролем правоохранительных органов. Основным практическим препятствием является разобщенность правоохранительного реагирования на опасности и угрозы, которые исходят от преступного использования технологий ИИ. Преодоление подобных преград несет за собой не только трансформацию законодательства по новым цифровым технологиям, но и полноценную ревизию всех задач и функциональных возможностей субъектов защиты от киберпреступности. Считаем, что назрела насущная потребность в создании нового, более технически и организационно оснащенного правоохранительного органа для эффективного отражения кибератак и защиты от высокотехнологической преступности во всех сферах жизнедеятельности нашего общества, где защита будет приоритетом не после совершения преступного деяния, а в процессе создания и реализации новых цифровых технологических решений.

---

[6] *Простосердов М. А.* Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. ... канд. юрид. наук. М., 2016. С. 55 ; Цит. по : Информационный ресурс China Space // URL: http://www.chinaspace.ru/internet-tolko-po-pasportu/ (дата обращения: 06.01.2013).

БИБЛИОГРАФИЯ

1. *Простосердов М. А.* Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : дис. ... канд. юрид. наук. — М., 2016. — 232 с.
2. *Созанкова Е.* Дипфейки: как нейросети копируют реальность // URL: https://ru.wikipedia.org/wiki/Deepfake#mw-head (дата обращения: 14.08.2020).

Материал поступил в редакцию 7 декабря 2020 г.

REFERENCES

1. Prostoserdov MA. Ekonomicheskie prestupleniya, sovershaemye v kiberprostranstve, i mery protivodeystviya im : dis. ... kand. yurid. nauk [Economic crimes committed in cyberspace, and measures of counteraction to them:Cand. Sci. (Law)]. Moscow; 2016 (In Russ.).
2. Sozankova E. Dipfeyki: kak neyroseti kopiruyut realnost [Deepfakes: how neural networks copy reality]. Available from: https://ru.wikipedia.org/wiki/Deepfake#mw-head (accessed: 14 Aug 2020) (In Russ.).