https://doi.org/10.17816/RJLS50014

Искусственный интеллект в борьбе с экстремизмом

Бычков Василий Васильевич,
кандидат юридических наук, доцент,
декан факультета повышения квалификации Московской академии
Следственного комитета Российской Федерации
E-mail: bychkov_vasilij@bk.ru

Прорвич Владимир Антонович,
доктор юридических наук,
доктор технических наук, профессор,
профессор кафедры уголовного процесса Московской академии
Следственного комитета Российской Федерации
E-mail: kse60@mail.ru

Аннотация. *В статье раскрывается основная нормативная база по применению искусственного интеллекта в России. Анализируется возможность использования искусственного интеллекта в борьбе с преступностью. Формулируется необходимость применения искусственного интеллекта при создании компьютерной криминалистики для повышения эффективности выявления, раскрытия и расследования преступлений экстремистской направленности, совершенных с применением современных информационных технологий.*

Ключевые слова: *экстремизм, преступления экстремистской направленности, противодействие, выявление, раскрытие, расследование, предупреждение, искусственный интеллект, компьютерная криминалистика.*

В настоящее время словосочетание «искусственный интеллект» (ИИ; англ. artificial intelligence, AI) ни у кого не вызывает недоумение. Все свыклись с мыслью о возможности слияния «машинного» и человеческого разума. Это понятие основательно вошло из фантастики в нашу повседневную действительность. В Послании к Федеральному Собранию 15.01.2020 Президент Российской Федерации В.В. Путин отметил: «Сегодня скорость технологических изменений в мире многократно возрастает, и мы должны создать собственные технологии и стандарты по тем направлениям, которые определяют будущее. Речь прежде всего об искусственном интеллекте, генетике, новых материалах, источниках энергии, цифровых технологиях»[1].

К настоящему времени уже создана отечественная нормативная база, на которую опирается применение искусственного интеллекта в различных сферах общественных отношений. Более того, Россия вошла в число стран, имеющих документы стратегического планирования в сфере искусственного интеллекта [1, с. 171–185; 2, с. 69–89; 3, с. 7–18]. В частности, в Стратегии научно-технологического развития Российской Федерации[2] одним из приоритетных направлений определен искусственный интеллект. В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы[3] искусственный интеллект назван в числе основных направлений развития российских информационных и коммуникационных технологий. Введен в действие ГОСТ Р 43.0.8-2017 «Информационное обеспечение техники и операторской деятельности. Искусственно-интеллектуализированное человекоинформационное взаимодействие. Общие положения»[4], утвержденный Приказом Федерального агентства по техническому регулированию и метрологии от 27.07.2017 № 757-ст.

Национальной стратегией развития искусственного интеллекта на период до 2030 года

[1] Послание Президента Федеральному Собранию. URL: http://kremlin.ru/events/president/news (дата обращения: 12.11.2020).

[2] Утверждена Указом Президента РФ от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации» // Собрание законодательства РФ. 2016. № 49. Ст. 6887.

[3] Утверждена Указом Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

[4] Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200146327 (дата обращения: 12.11.2020).

(далее — Стратегия развития искусственного интеллекта) определяются цели и основные задачи развития искусственного интеллекта в Российской Федерации, а также меры, направленные на его использование в целях обеспечения национальных интересов и реализации стратегических национальных приоритетов[5].

С 1 июля 2020 г. на ближайшие пять лет запланировано проведение эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве, а также последующего возможного использования результатов применения искусственного интеллекта[6].

Чтобы определить основные подходы к трансформации системы нормативного регулирования в Российской Федерации и обеспечить возможности создания и применения современных информационных технологий в различных сферах экономики с соблюдением прав граждан и обеспечением безопасности личности, общества и государства, создать предпосылки для формирования основ правового регулирования новых общественных отношений, складывающихся в связи с разработкой и применением технологий искусственного интеллекта и робототехники и систем на их основе, а также для выявления правовых барьеров, препятствующих разработке и применению указанных систем, была разработана Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года[7].

Под искусственным интеллектом, согласно Стратегии развития искусственного интеллекта, понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений. По утверждению специалистов, разработки в сфере искусственного интеллекта ведутся по двум направлениям: нейрокибернетическому и логическому. Первое занимается созданием универсального интеллекта, по сути, аналога человеческого мозга, способного решать любые интеллектуальные задачи без участия человека, а второе направлено на создание прикладного искусственного интеллекта, нацеленного на решение одной или несколько прикладных задач [4, с. 2].

В настоящее время существующая нормативная база и основная масса научных исследований по искусственному интеллекту направлены на повышение эффективности экономики [5; 6, с. 201–207] и улучшение социальной сферы.

В Стратегии развития искусственного интеллекта указано, что использование технологий искусственного интеллекта в отраслях экономики носит общий («сквозной») характер и способствует созданию условий для улучшения эффективности и формирования принципиально новых направлений деятельности хозяйствующих субъектов, в том числе за счет:

- повышения эффективности процессов планирования, прогнозирования и принятия управленческих решений (включая прогнозирование отказов оборудования и его превентивное техническое обслуживание, оптимизацию планирования поставок, производственных процессов и принятия финансовых решений);
- автоматизации рутинных (повторяющихся) производственных операций;
- использования автономного интеллектуального оборудования и робототехнических комплексов, интеллектуальных систем управления логистикой;
- повышения безопасности сотрудников при выполнении бизнес-процессов (включая прогнозирование рисков и неблагоприятных событий, снижение уровня непосредственного участия человека в процессах, связанных с повышенным риском для его жизни и здоровья);
- повышения лояльности и удовлетворенности потребителей (в том числе направление им персонализированных предложений и рекомендаций, содержащих существенную информацию);

[5] Утверждена Указом Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

[6] Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона „О персональных данных“» // Собрание законодательства РФ. 2020. № 17. Ст. 2701.

[7] Утверждена Распоряжением Правительства РФ от 19.08.2020 № 2129-р // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru (дата обращения: 12.11.2020).

- оптимизации процессов подбора и обучения кадров, составления оптимального графика работы сотрудников с учетом различных факторов.

Использование технологий искусственного интеллекта в социальной сфере способствует созданию условий для повышения уровня жизни населения, в том числе за счет:

- повышения качества услуг в сфере здравоохранения (включая профилактические обследования, диагностику, основанную на анализе изображений, прогнозирование возникновения и развития заболеваний, подбор оптимальных дозировок лекарственных препаратов, сокращение угроз пандемий, автоматизацию и точность хирургических вмешательств);
- повышения качества услуг в сфере образования (включая адаптацию образовательного процесса к потребностям обучающихся и потребностям рынка труда, системный анализ показателей эффективности обучения для оптимизации профессиональной ориентации и раннего выявления детей с выдающимися способностями, автоматизацию оценки качества знаний и анализа информации о результатах обучения);
- повышения качества предоставления государственных и муниципальных услуг, а также снижения затрат на их предоставление.

Однако с помощью искусственного интеллекта могут быть совершены как общеуголовные преступления, так и преступления экстремистской и террористической направленности [7, с. 172]:

- террористический акт (ст. 205 УК РФ), который может выражаться как в совершении взрыва, поджога, отравлении источника водоснабжения, лишении жизни людей с использованием робототехники;
- вандализм (ст. 214 УК РФ): легко себе представить использование БПЛА[8], переносящего капсулу с краской и сбрасывающего ее на здание или сооружение для их осквернения;
- приведение в негодность объектов жизнеобеспечения (ст. 215.2 УК РФ) путем их разрушения, повреждения или приведение иным способом в негодное для эксплуатации состояние с помощью роботов. Совершение этих действий из корыстных или хулиганских побуждений квалифицируется по ст. 215.2 УК РФ; при отсутствии названных мотивов, но при наличии цели подрыва экономической безопасности и обороноспособности РФ — по ст. 282 УК РФ;
- незаконное проникновение на подземный или подводный объект, охраняемый в соответствии с законодательством Российской Федерации о ведомственной или государственной охране, с использованием робототехники, включая БПЛА (ст. 215.4 УК РФ);
- хищение ядерных материалов или радиоактивных веществ путем применения робототехники для незаконного проникновения в помещение или хранилища и завладения предметом преступления (ст. 221 УК РФ);
- незаконное приобретение, передача, сбыт, хищение оружия, его основных частей, боеприпасов, взрывчатых веществ, взрывных устройств (ст. 222, 222.1, 226 УК РФ), а также его незаконное перемещение через Таможенную границу Таможенного союза в рамках ЕврАзЭС либо государственную границу РФ государствами — членами Таможенного союза в рамках ЕврАзЭС (ст. 226.1 УК РФ) с использованием робототехники, особенно БПЛА;
- нападение на морское или речное судно в целях завладения чужим имуществом, совершенное с применением насилия либо с угрозой его применения посредством использования робототехники, включая БПЛА (ст. 227 УК РФ).

Преимущества в использовании искусственного интеллекта для совершения преступлений очевидны:

- во-первых, возможность его применения в опасных зонах, в том числе биологически опасных;
- во-вторых, физическая безопасность лица, использующего эти технологии для совершения преступления, поскольку оно находится, как правило, далеко от места его использования, у него нет страха быть обнаруженным, что психологически облегчает принятие решений, связанных с нарушением общественно опасных деяний;
- в-третьих, по использованному искусственному интеллекту трудно идентифицировать преступника.

Необходимо учитывать, что искусственный интеллект предлагает определенные решения в соответствии с тем алгоритмом, который был реализован в компьютерной программе, написанной и отлаженной одним или несколькими программистами. Понятно, что если посредством или с участием такой программы, используемой в качестве искусственного интеллекта, совершается преступление, то речь идет об умышленной форме вины, так как механизм или устройство действует, выполняя волю создателя программы. Это предполагает опосредованное совершение преступления [8, с. 2].

С точки зрения уголовного права необходимо выделять случаи, когда при разработке

[8] Беспилотный летательный аппарат (в разговорной речи также «беспилотник» или «дрон», от англ. drone — трутень) — летательный аппарат без экипажа на борту. См.: Большая Российская энциклопедия. М., 1994. С. 108.

алгоритма и создания компьютерной программы искусственного интеллекта соответствующие лица не предполагали причинения какого-либо вреда любым другим лицам, юридическим лицам, государству и обществу. При этом в некоторых случаях возможно возникновение следующих непредвиденных ситуаций, когда результаты обработки определенной информации данным вариантом искусственного интеллекта существенно отличаются от ожидаемых разработчиками соответствующей компьютерной программы:

- алгоритм, по которому написана компьютерная программа, предназначен для сочинения музыки на основе выборки определенных музыкальных фраз, мелодий, их сочетания в оригинальной последовательности и т.д. Результат применения подобной программы ее автором может привести к совершению преступления, которое предусмотрено ч. 1 ст. 146 УК РФ либо ст. 272 УК РФ;
- создан искусственный интеллект, предполагающий саморазвитие и самостоятельное мышление, с выходом за рамки первоначальной программы. При этом нет гарантии, что при совершении таким искусственным интеллектом деяния оно не подпадет под признаки состава преступления;
- искусственный интеллект сам создает новый искусственный интеллект, который совершает общественно опасное деяние.

Вполне очевидно, что процессы разработки алгоритмов искусственного интеллекта, создания и применения соответствующих компьютерных программ выдвигают на первый план ряд актуальных задач по их уголовно-правовому регулированию, способному не только спрогнозировать риски их применения, но и предусмотреть ответственность в случае причинения вреда общественным отношениям. Существует отставание в разработке, в частности, уголовно-правовых норм, поскольку не завершен процесс определения гражданско-правового статуса робота, а от него зависит построение концепции уголовно-правовых рисков в искусственном интеллекте.

Специалистами предлагается проработать вопрос об уголовной ответственности за незаконный оборот робототехники с искусственным интеллектом; грубое нарушение правил эксплуатации роботов, повлекшее причинение вреда жизни, здоровью человека или крупного ущерба. Подобные нормы будут априори содержать бланкетные диспозиции, их принятие потребует сначала разработки соответствующего отраслевого законодательства, определяющего правила оборота робототехники, способной причинить существенный вред общественным отношениям, установления запрета и (или) ограничения в обороте отдельных видов робототехники, например, смертоносных автономных систем хотя бы частными лицами, и т.д. В качестве условий законного оборота такой техники производитель должен предусмотреть возможность аутентификации робота, ведение реестра пользователей или владельцев роботов [7, с. 178].

С целью внедрения искусственного интеллекта в юриспруденцию специалистами выделяются следующие его особенности:

- многозадачность;
- способность работы с большим массивом информации;
- стабильность системы и надежность сохранения данных;
- гибкость системы, способность к самообучению;
- способность анализировать правовые ситуации с постоянно меняющимися условиями [9, с. 215].

Искусственный интеллект уже получил определенное применение и в судебной системе, в том числе при подготовке процессуальных документов и работе с ними. В частности, уже сейчас в судебной практике действует программа «Casebook», основанная на технологии «machine learning». С ее помощью создается возможность определения исхода дела (с определенной вероятностью). При подаче искового заявления в суд с ее помощью истец может определить вероятность решения суда в его пользу и на основании этого разработать тактику своего участия в деле.

Внедрение программ искусственного интеллекта в делопроизводство позволяет оптимизировать работу с огромным массивом входящих и исходящих документов, снижает трудоемкость их обработки и тем самым расширяет возможности судей для более глубокого изучения материалов каждого дела и повышения качества обоснования принимаемого решения.

Следует отметить, что Европейской комиссией по вопросам эффективности правосудия (CEPEJ) в 2018 г. принята Этическая хартия использования искусственного интеллекта в судебных системах, в которой названы приоритетные принципы использования искусственного интеллекта [10, с. 23].

В настоящее время системы искусственного интеллекта применяются в оперативно-розыскных действиях, дознании и расследовании уголовных дел, включая использование при этом специальных знаний в различной форме. Отмечается их использование учеными и специалистами при проведении исследований и разработок в рамках криминологии и криминалистики. Известны и предложения по их использованию для противодействия

киберугрозам и террористическим угрозам государству и обществу [11, с. 10]. Среди них можно выделить следующие:

- формирование уникальной системы психологических и иных признаков преступника по результатам обработки и систематизации имеющихся сведений о нем; моделирование его преступного поведения для обоснования выводов о возможности совершения им нового преступления и даже определения его возможного времени, места и способа;
- анализ «больших данных», полученных по результатам видеонаблюдения мест возможного пребывания преступника, с целью идентификации его личности и возможных контактов с сообщниками;
- формирование визуальных текстовых материалов — ориентировок по разыскиваемым лицам;
- сортировка правдивых и ложных сведений о фактах и обстоятельствах, имеющих значение для установления истины по расследуемому уголовному делу, в вербальной информации, полученной в ходе допросов подозреваемых, свидетелей и иных лиц;
- выявление ложных сведений в документах различного вида — как на бумажных, так и на электронных носителях;
- отслеживание и трассировка интернет-трафика подозреваемых лиц в сети Интернет и коммуникаций между подозреваемыми лицами в сети Интернет, в мессенджерах[9];
- расшифровка закодированной информации, в том числе при групповой обработке материалов уголовного дела, для выявления замаскированных идеальных следов преступлений [12, с. 25].

Искусственный интеллект широко применяется и для обработки различных статистических данных, оказания помощи в составлении документов, насыщения сайтов правоохранительных органов правовой информацией, принятия решений о квалификации преступных деяний [10, с. 25].

В настоящее время подавляющее большинство преступлений экстремистской направленности (публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ), публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 280.1 УК РФ), возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ), организация экстремистского сообщества (ст. 282.1 УК РФ), организация деятельности экстремистской организации (ст. 282.2 УК РФ), финансирование экстремистской деятельности (ст. 282.3 УК РФ), а также другие преступления, совершаемые по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы) совершаются с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет [13–17].

Кроме этого, интернет-технологии применяются и при совершении ряда других преступлений, нацеленных на совершение самоубийства:

- доведение до самоубийства (п. «д» ч. 2 ст. 110 УК РФ). К примеру, в Тюменской области вынесен приговор создателю «группы смерти» во «ВКонтакте» Филиппу Будейкину, который с помощью соцсети пытался довести до самоубийства двух несовершеннолетних девочек. При этом в ходе расследования Будейкин проверялся на причастность к гибели более пятнадцати подростков по всей России[10];
- склонение к совершению самоубийства или содействие совершению самоубийства (п. «д» ч. 3 ст. 110.1 УК РФ). Так, куратор «группы смерти» «Синий кит», финансовый аналитик из Московской области Никита Неаронов приговорен в Челябинске к реальному сроку в колонии общего режима. Он через интернет-приложение систематически оказывал психологическое воздействие на потерпевших с целью доведения их до самоубийства, призывая их к нанесению ран на своем теле, давая обязательные к исполнению задания, заключавшиеся в прослушивании и просмотре аудио-и видеоматериалов со сценами насилия, суицидов, и тем самым формировал депрессивную направленность сознания[11]; гр-ка Ганиева Ф.М., используя социальную сеть «ВКонтакте» информационно-телекоммуникационной сети Интернет,

[9] Мессенджер (система обмена сообщениями в режиме реального времени, "...времени, англ. Instant..." англ. Instant messaging, IM) — службы мгновенных сообщений (Instant Messaging Service, IMS), программы онлайн-консультанты (OnlineSaler) и программы-клиенты (Instant Messenger, IM), с помощью которых могут передаваться текстовые сообщения, звуковая информация, фото и видеоизображения, производиться такие действия, как совместное создание графических документов и т.п.

[10] Администратор «групп смерти» получил три года. URL: https://www.gazeta.ru/tech/2017/07/18_a_10793984.shtml (дата обращения: 12.11.2020).

[11] Суд в Челябинске приговорил куратора группы «Синий кит» к реальному сроку. URL: https://www.znak.com/2020-05-27/sud_v_chelyabinske_prigovoril_kuratora_gruppy_siniy_kit_k_realnomu_sroku (дата обращения: 12.11.2020).

склонила знакомую несовершеннолетнюю к совершению самоубийства[12];

- организация деятельности, направленной на побуждение к совершению самоубийства (ч. 2 ст. 110.2 УК РФ). Например, в августе 2017 г. Ш. организовала в социальной сети «ВКонтакте» «игру», суть которой сводилась к выполнению несовершеннолетними заданий, направленных на причинение себе телесных повреждений, подавления психики ребенка и окончание игры путем совершения самоубийства. Она привлекла к реализации замысла своего брата Г., который добровольно согласился оказывать ей помощь в отыскании в социальной сети «ВКонтакте» потенциальных участников «игры» («китов») — подростков, находящихся в тяжелой жизненной ситуации, направлять их поведение. Суд признал Ш. виновной в совершении преступлений, предусмотренных п. «а, в, г, д» ч. 3 ст. 110.1 и ч. 2 ст. 110.2 УК РФ, Г. — в совершении преступления, предусмотренного п. «а, г, д» ч. 3 ст. 110.1 УК РФ[13].

Особую опасность представляют публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ч. 2 ст. 205.2 УК РФ). Так, М., отбывая наказание в ИК-5 УФСИН России по Орловской области, используя смартфон, имеющий доступ к сети Интернет, разместил на своей странице в социальной сети «ВКонтакте» аудиофайлы, содержащие публичные призывы к осуществлению террористической деятельности и публичное оправдание терроризма. В июле 2019 г. Московским окружным военным судом он признан виновным в совершении преступления, предусмотренного ч. 2 ст. 205.2 УК РФ[14].

Аналогичный вывод можно сделать и в отношении организации деятельности террористической организации и участия в деятельности такой организации (ст. 205.5 УК РФ).

Анализ опубликованных материалов по рассматриваемым проблемам показывает, что все чаще экстремистская пропаганда используется различными зарубежными террористическими организациями. Чаще всего они используют для этого веб-сайты с парольной защитой[15], а также ограниченные для доступа в Интернете чат-группы[16], в том числе как средство тайной вербовки своих новых сторонников. При этом для новых членов таких группировок интернет-форумы[17] ограниченного доступа становятся источником запрещенной информации о террористических организациях и инструкций для подготовки к непосредственным действиям террористического характера, в том числе по экстремистским мотивам[18]. Так, в феврале текущего года в г. Симферополе Республики Крым под стражу были заключены два подростка 16 и 17 лет, планировавшие совершение терактов в образовательных учреждениях Крыма. Данные подростки состояли в неонацистском интернет-сообществе, членом которого ранее был Владислав Росляков, устроивший в октябре 2018 г. стрельбу в колледже в Керчи[19].

Не меньшую опасность представляет интернет-деятельность по организации массовых беспорядков (ст. 212 УК РФ). Так, в июле 2019 г. в Москве прошли массовые беспорядки. Причиной проведения митинга послужил отказ в регистрации нескольким кандидатам в депутаты Мосгордумы. Было установлено, что за ними числятся подписи уже умерших людей. Кандидаты не стали обжаловать решения избирательных комиссий в установленном порядке и начали через Интернет призывать граждан принять участие в противозаконном митинге, «заведомо допуская, что данные действия

[12] Приговор Судакского городского суда Республики Крым от 07.05.2018 № 1-25/2018 по делу № 1-25/2018. URL: https://sudact.ru/regular/doc/AnhCjvSdlpdj/ (дата обращения: 12.11.2020).

[13] Приговором Собинского городского суда брат и сестра осуждены за вовлечение несовершеннолетних в интернет-игру суицидальной направленности. URL: http://oblsud.wld.sudrf.ru/modules.php?name=press_dep&op=1&did=1528 (дата обращения: 12.11.2020).

[14] Апелляционное определение № 208-АПУ18-3 // Обзор судебной практики Верховного Суда Российской Федерации № 3 (2018), утвержденный Президиумом Верховного Суда РФ 14.11.2018 (ред. от 26.12.2018) // СПС КонсультантПлюс.

[15] Веб-сайт, или сайт (от англ. website: web — «паутина, сеть» и site — «место», буквально «место, сегмент, часть в сети») — одна или несколько логически связанных между собой веб-страниц; также место расположения контента сервера. Обычно сайт в Интернете представляет собой массив связанных данных, имеющий уникальный адрес и воспринимаемый пользователями как единое целое.

[16] Чат (от англ. chatter — болтать) — средство обмена сообщениями по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение.

[17] Интернет-форум, или веб-форум — интернет-сервис (платформа) для общения между пользователями Интернета (более двух участников) на одну тему или на несколько тем (зависит от специализации форума).

[18] Использование Интернета в террористических целях. Вена: Организация Объединенных Наций, 2013. URL: https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf (дата обращения: 12.11.2020).

[19] Суд арестовал подозреваемых в подготовке теракта в Керчи подростков. URL: https://www.rbc.ru/rbcfreenews/5e4ec7ca9a7947721f98dc80 (дата обращения: 12.11.2020).

могут спровоцировать массовые беспорядки». В результате этого участники несогласованной акции, находясь в центре Москвы, игнорируя законные требования представителей власти, грубо нарушая общественный порядок, применили насилие в отношении представителей власти, прорвали оцепление и, выйдя на проезжую часть, парализовали движение автотранспорта на Садовом кольце, а также совершили иные противоправные действия[20].

В последнее время особую актуальность приобрели проблемы выявления и пресечения высокотехнологичных преступлений, связанных с реабилитацией нацизма (ст. 354.1 УК РФ). Так, в отношении нескольких граждан Следственным комитетом РФ возбуждены уголовные дела за размещение в Интернете во время акции «Бессмертный полк онлайн» фотографий нацистов. Верховный суд РФ признал законным приговор жителю Перми Владимиру Лузгину, осужденному за размещение в Интернете материалов, в которых одобрялась деятельность украинского националиста Степана Бандеры[21].

Наиболее наглядно использование Интернета в экстремистских целях можно наблюдать буквально в режиме реального времени по событиям в Республике Беларусь. Так, в социальных сетях было создано сообщество «Партизаны Могилева», пользователи которого собирались в заброшенном помещении в лесу под Могилевом и отрабатывали тактику ведения уличных боев, захвата помещений, штурмового альпинизма и ведения боевых действий в лесу[22]. Оппозиция белорусского Президента, находящаяся в Польше и Литве, посредством «Телеграма»[23] координирует действия митингующих, диктует им инструкции по совершению беспорядков, угрожает обрушением налоговой системы страны и обвалом государственной валюты, а гражданам, отказывающимся протестовать, угрожает выложить в общий доступ их установочные данные и все сведения о них[24], а затем и осуществляет свои угрозы.

Проведенный анализ показывает, что современные информационные технологии, включая элементы искусственного интеллекта, стали вполне привычным инструментарием экстремистов. Более того, по многим преступлениям рассматриваемого вида намечаются опасные тенденции «интеллектуального опережения» преступниками представителей правоохранительных органов. Это выдвигает на первый план и делает сверхактуальными задачи по форсированному развитию научных основ компьютерной криминалистики по преступлениям экстремистской направленности, связанным с применением высокотехнологичного инструментария.

В этой связи необходимо обратить внимание на то, что в соответствии с Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» была принята национальная программа «Цифровая экономика Российской Федерации»[25], в составе которой был детально разработан паспорт национального проекта «Цифровая экономика Российской Федерации»[26]. Среди задач данного проекта указаны создание системы правового регулирования цифровой экономики, основанной на гибком подходе к каждой сфере, внедрение гражданского оборота на базе цифровых технологий, а также обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства.

Для решения этих и других задач в данный национальный проект был включен ряд федеральных проектов. При этом Правительству Российской Федерации было поручено до 15 декабря 2019 г. обеспечить внесение изменений в национальную программу «Цифровая экономика Российской Федерации», в том числе разработать и утвердить федеральный проект

[20] Суд арестовал В. Костенка по делу об участии в массовых беспорядках в Москве 27 июля (дополнение). URL: https://www.mskagency.ru/materials/2917207 (дата обращения: 12.11.2020).

[21] Верховный суд РФ признал законным приговор, вынесенный жителю Перми за реабилитацию нацизма. URL: https://www.kommersant.ru/doc/3078015 (дата обращения: 12.11.2020).

[22] В Белоруссии снова появились партизаны. URL: https://eadaily.com/ru/news/2020/09/14/v-belorussii-snova-poyavilis-partizany (дата обращения: 12.11.2020).

[23] Телеграм (telegram) — кроссплатформенный мессенджер, позволяющий обмениваться сообщениями и медиафайлами многих форматов. Пользователи могут отправлять сообщения и обмениваться фотографиями, стикерами, голосовыми сообщениями, файлами любого типа, а также делать аудио- и видеозвонки.

[24] Белоруссия потребовала от Польши выдать основателей Telegram-канала HEXTA. URL: https://www.rbc.ru/politics/16/11/2020/5fb286059a794701311b1294 (дата обращения: 12.11.2020).

[25] Утверждена Президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24.12.2018 № 16 // СПС КонсультантПлюс.

[26] Утвержден протоколом заседания Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 04.06.2019 № 7 // СПС КонсультантПлюс.

«Искусственный интеллект»[27]. Кроме этого, предусмотрено внесение изменений в Уголовный кодекс РФ, связанных с криминализацией новых типов деяний, совершенных с использованием современной компьютерной техники и информационных технологий, а также обеспечением защиты прав и законных интересов личности, общества и государства от новых угроз, возникающих при переходе к новому, информационному обществу и экономике знаний. При этом необходимо обратить внимание на запланированное создание в 2020 г. системы негосударственных экспертных организаций в области компьютерной криминалистики, ответственность за которое было возложено на МВД России и Минюст России.

По нашему мнению, создание нового направления криминалистики, связанного с борьбой с современной высокотехнологичной преступностью, не может быть сориентировано исключительно на защиту цифровой экономики. Кроме того, ориентация на создание соответствующих средств борьбы с криминалом, включая использование искусственного интеллекта, силами негосударственных экспертных организаций, под эгидой МВД России и Минюста России, не позволит обеспечить выведение на качественно новый уровень всей системы уголовно-правовой защиты прав и законных интересов граждан, организаций, государства и общества в целом от атак высокотехнологичного криминала.

Необходима мобилизация лучших ученых и специалистов, разрабатывающих проблемы борьбы с высокотехнологичным криминалом во всех сферах общественных отношений. Поскольку речь идет об обеспечении безопасности в переходных условиях к новому, информационному обществу, когда постоянно возникают нетиповые задачи, работа ученых должна быть подкреплена организационными мероприятиями высокого уровня. Прежде всего, следует обратить внимание на тот научный потенциал, который создан в государственных образовательных учреждениях, готовящих кадры высшей квалификации для правоохранительных органов. Соответствующая программа действий, сформулированная в недавно вышедшей монографии [18] применительно к созданию компьютерной криминалистики для раскрытия и расследования преступлений в сфере традиционной и цифровой экономики, может быть принята за основу и для разработки подобной программы применительно к преступлениям экстремистской направленности, совершаемым с помощью современных информационных технологий.

Мероприятия, выполняемые в рамках такой программы, должны быть нацелены не только на конкретные способы применения искусственного интеллекта для обнаружения и идентификации признаков политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо ненависти или вражды в отношении какой-либо социальной группы. Их значительная часть может быть сориентирована и на оперативную передачу в специализированные подразделения правоохранительных органов данных о распространителях преступной информации и ее пользователях. Это, кстати, позволит избежать общей блокировки мессенджеров[28].

Вместе с тем, значительная часть таких мероприятий должна быть сориентирована на создание интегрированного научного фундамента компьютерной криминалистики, чтобы объединить в борьбе с современным криминалом в данной сфере возможности всех наук уголовно-правового блока — уголовного права, уголовно-процессуального права, криминалистики, оперативно-розыскной деятельности и судебной экспертизы.

Список литературы

1. Незнамов А.В. О концепции регулирования технологий искусственного интеллекта и робототехники в России // Закон. 2020. № 1. С. 171–185.
2. Незнамов А.В., Наумов В.Б. Стратегия регулирования робототехники и киберфизических систем // Закон. 2018. № 2. С. 69–89.
3. Ручкина Г.Ф. Искусственный интеллект, роботы и объекты робототехники: к вопросу о теории правового регулирования в Российской Федерации // Банковское право. 2020. № 1. С. 7–18.
4. Андреев В.К. Динамика правового регулирования применения искусственного интеллекта // Журнал российского права. 2020. № 3. С. 58–68.

[27] Утверждена Указом Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

[28] Напр., Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзором) с 16.04.2018 по 18.06.2020 был заблокирован Telegram в России, в соответствии с двумя законами, имеющими антитеррористическую направленность, так называемым пакетом Яровой: Федеральными законами от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму“ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» и № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

5. Волынский А.Ф., Прорвич В.А. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография. М.: Экономика, 2019. 364 с.
6. Прорвич В.А. Особенности комплексного применения специальных знаний для профилактики преступлений в сфере традиционной и цифровой экономики // Вестник экономической безопасности. 2020. № 2. С. 201–207.
7. Грачева Ю.В., Арямов А.А. Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. № 6. С. 169–178.
8. Денисов Н.Л. Концептуальные основы формирования международного стандарта при установлении уголовной ответственности за деяния, связанные с искусственным интеллектом // Международное уголовное право и международная юстиция. 2019. № 4. С. 18–20.
9. Закиров Р.Ф. Использование современных IT-технологий как средство достижения основных задач судопроизводства // Вестник гражданского процесса. 2018. № 1. С. 211–219.
10. Сушина Т.Е., Собенин А.А. Перспективы и риски использования искусственного интеллекта в уголовном судопроизводстве // Российский следователь. 2020. № 6. С. 21–25.
11. Мохат П.М. Возможности, особенности и условия применения искусственного интеллекта в юридической практике // Администратор суда. 2018. № 2. С. 8–12.
12. Организация и методика расследования отдельных видов экономических преступлений: учебно-методическое пособие / Под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М.: «Спутник+», 2016. 624 с.
13. Бычков В.В. Противодействие преступлениям экстремистской направленности: курс лекций. М.: Юрлитинформ, 2013. 256 с.
14. Бычков В.В. Противодействие преступлениям экстремистской и террористической направленности: криминологические, уголовно-правовые и криминалистические аспекты: монография / В.В. Бычков, Р.А. Сабитов, Т.Р. Сабитов. М.: Юрлитинформ, 2013. 363 с.
15. Бычков В.В. Преступления экстремистской направленности: понятие, классификация, общие объективные и субъективные признаки, квалифицированные составы // Расследование преступлений: проблемы и пути их решения. 2018. № 4(22). С. 36–41.
16. Багмет А.М. Расследование преступлений, связанных с экстремистской и террористической деятельностью: учебник / А.М. Багмет, В.В. Бычков, Ю. М. Зеленков. М.: ЮНИТИ-ДАНА, 2019. 719 с.
17. Бычков В.В., Ротов В.А. Понятие и виды преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей // Расследование преступлений: проблемы и пути их решения. 2020. № 3. С. 26–31.
18. Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: монография. М.: Экономика, 2020. 476 с.

Artificial Intelligence in the Fight Against Extremism

Bychkov Vasily,
Candidate of Law Science,
Associate Professor,
Dean of the Faculty of Excellence of the Moscow Academy
of the Investigative Committee of the Russian Federation
E-mail: bychkov_vasilij@bk.ru

Prorvich Vladimir,
Doctor of Law Science,
Doctor of Technical Science, Professor,
Professor of the Department of Criminal Procedure
of the Moscow Academy of the Investigative Committee
of the Russian Federation
E-mail: kse6o@mail.ru

Abstract. *The article reveals the basic regulatory framework for the use of artificial intelligence in Russia. The possibility of using artificial intelligence to fight crime is being analyzed. The need for artificial intelligence to create computer forensic in countering extremist crimes is in development.*
Keywords: *Extremism, extremist crimes, countering, identify, investigation, warning, artificial intelligence, computer forensics.*

References

1. Neznamov A.V. O koncepcii regulirovaniya tekhnologij iskusstvennogo intellekta i robototekhniki v Rossii. *Zakon*. 2020;(1):171-185. (In Russ.).
2. Neznamov A.V., Naumov V.B. Strategiya regulirovaniya robototekh-niki i kiberfizicheskih system. *Zakon*. 2018;(2):69-89. (In Russ.).
3. Ruchkina G.F. Iskusstvennyj intellekt, roboty i ob"ekty roboto-tekhniki: k voprosu o teorii pravovogo regulirovaniya v Rossijskoj Federacii. *Bankovskoe pravo*. 2020;(1):7-18. (In Russ.).
4. Andreev V.K. Dinamika pravovogo regulirovaniya primeneniya iskusstvennogo intellekta. *Journal of Russian Law*. 2020;(3)58-68. (In Russ.).
5. Volynskij A.F., Prorvich V.A. Elektronnoe sudoproizvodstvo po prestupleniyam v sfere ekonomiki (nauchno-prakticheskie aspekty). Moscow: Ekonomika, 2019. (In Russ.). 364 p. (In Russ.).
6. Prorvich V.A. Osobennosti kompleksnogo primeneniya special'nyh znanij dlya profilaktiki prestuplenij v sfere tradicionnoj i cifrovoj ekonomiki. *Vestnik ekonomicheskoj bezopasnosti*. 2020;(2):201-207. (In Russ.).
7. Gracheva Yu.V., Aryamov A.A. Robotizaciya i iskusstvennyj intellekt: ugolovno-pravovye riski v sfere obshchestvennoj bezopasnosti. *Aktual'nye problemy rossijskogo prava*. 2020;(6):169-178. (In Russ.).
8. Denisov N.L. Konceptual'nye osnovy formirovaniya mezhdunarodnogo standarta pri ustanovlenii ugolovnoj otvetstvennosti za deyaniya, svyazannye s iskusstvennym intellektom. *Mezhdunarodnoe ugolovnoe pravo i mezhdunarodnaya yusticiya*. 2019;(4):18-20. (In Russ.).
9. Zakirov R.F. Ispol'zovanie sovremennyh IT-tekhnologij kak sredstvo dostizheniya osnovnyh zadach sudoproizvodstva. *Vestnik grazhdanskogo processa*. 2018;(1):211-219. (In Russ.).
10. Sushina T.E., Sobenin A.A. Perspektivy i riski ispol'zovaniya iskusstvennogo intellekta v ugolovnom sudoproizvodstve. *Rossijskij sledovatel'*. 2020;(6):21-25. (In Russ.).
11. Morhat P.M. Vozmozhnosti, osobennosti i usloviya primeneniya iskusstvennogo intellekta v yuridicheskoj praktike. *Administrator suda*. 2018;(2):8-12.
12. Organizaciya i metodika rassledovaniya otdel'nyh vidov ekonomicheskih prestuplenij: manual. Pod red. A.I. Bastrykina, A.F. Volynskogo, V.A. Prorvicha. Moscow: «Sputnik+», 2016. (In Russ.) 624 p. (In Russ.).
13. Bychkov V.V. Protivodejstvie prestupleniyam ekstremistskoj napravlennosti: kurs lekcij. Moscow: Yurlitinform, 2013. 256 p. (In Russ.).
14. Bychkov V.V. et al. Protivodejstvie prestupleniyam ekstremistskoj i terroristicheskoj napravlennosti: kriminologicheskie, ugolovno-pravovye i kriminalisticheskie aspekty: monografiya. Moscow: Yurlitinform, 2013. 363 p. (In Russ.).
15. Bychkov V.V. Prestupleniya ekstremistskoj napravlennosti: ponyatie, klassifikaciya, obshchie ob"ektivnye i sub"ektivnye priznaki, kvalificirovannye sostavy. *Rassledovanie prestuplenij: problemy i puti ih resheniya*. 2018;4(22):36-41. (In Russ.).
16. Bagmet A.M. et al. Rassledovanie prestuplenij, svyazannyh s ekstremistskoj i terroristicheskoj deyatel'nost'yu: uchebnik. Moscow: YUNITI-DANA, 2019. 719 p. (In Russ.).
17. Bychkov V.V., Rotov V.A. Ponyatie i vidy prestuplenij ekstremistskoj napravlennosti, sovershaemyh s ispol'zovaniem informacionno-telekommunikacionnyh setej. *Rassledovanie prestuplenij: problemy i puti ih resheniya*. 2020;(3):26-31. (In Russ.).
18. Volynskij A.F., Prorvich V.A. Komp'yuternaya kriminalistika v sisteme ugolovno-pravovoj zashchity «tradicionnoj» i cifrovoj ekonomiki. Moscow: Ekonomika, 2020. (In Russ.). 476 p. (In Russ.).