4. [Электронный ресурс]. – https://vpk.name/news/329623_kiberbezopasnost_po-izrailski.html. – Дата доступа: 25.10.2022.

5. Шеремет, И.А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере / И.А. Шеремет // Вопр. кибербезопасности. – 2016. – № 5 (18). – С. 3–7.

УДК 004.838

В.В. Комерцов

ТЕХНОЛОГИИ МАШИННОГО ОБУЧЕНИЯ КАК ИНСТРУМЕНТ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Основная цель настоящего исследования – систематизировать опыт в области правового регулирования создания и использования искусственного интеллекта (ИИ) и смежных технологий, а также выделить и осветить основные тенденции и ключевые проблемы в этой сфере в правоохранительной деятельности. Возможно, что результаты данного анализа поспособствуют формированию необходимой основы для выработки конкретных методологических и нормативных рекомендаций, как на национальном, так и на международном уровнях.

Приоритетные направления развития и использования технологий ИИ определяются в России с учетом национальных целей и стратегических задач, определенных Указом Президента Российской Федерации от 7 мая 2018 г. № 2042 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». Названные нормативно-правовые акты подчеркивают колоссальную государственную и общественную важность данной технологии в современной России [2].

Технологии ИИ постепенно охватывают современный мир. Технологии машинного обучения, основанные на обработке беспрецедентных массивов данных, выводят методы анализа информации на совершенно новый уровень, а робототехника выполняет действиями машин те задачи, которые раньше были прерогативой исключительно человека, потенциально делая жизнь людей более комфортной и создавая новые блага.

Закономерно, что технологические инновации, оказывающие такое глобальное воздействие на жизнь современного человека, несут в себе немалые риски. Осознание того, что технологии ИИ являются чрезвычайно сильными инструментами, способными принести обществу как большую пользу, так и серьезный вред, неизбежно приводит к мысли о

необходимости установления системы нормативных правил, принципов и ограничений, связанных с разработкой и применением систем с ИИ.

Феномен стремительного развития и распространения технологий ИИ далеко не всегда получает положительную оценку. С одной стороны, оптимистичный вариант развития ИИ предполагает органичное встраивание робототехнических устройств и сервисов ИИ в жизнь общества. С другой стороны, риски, исходящие от массового применения ИИ, порой рассматриваются как вызовы такого масштаба, который способен создать угрозу для самого существования человечества.

Безусловно, разработчики систем ИИ принимают ряд мер по минимизации рисков использования соответствующих технологий. Однако более глобальные риски социального, экономического и гуманитарного характера, как правило, намного труднее поддаются оценке [5].

Тем не менее представляется возможным выделить основные проблемные зоны индустрии ИИ, имеющие непосредственную связь с правом. Рассмотрим наиболее значимые, на наш взгляд, аспекты теоретических проблем правового регулирования разработки и применения ИИ и смежных технологий, которые обрели актуальность уже сегодня.

Развитие дискуссии о правовых аспектах ИИ и смежных технологий в значительной степени обусловлено ростом внимания к этическим проблемам машинного обучения и робототехники [4].

Само слово «робот» впервые появилось в научно-фантастической пьесе К. Чапека «R.U.R.» 1920 г., одной из центральных тем которой была этика использования мыслящих конструкторов в качестве рабочей силы. Впоследствии главным литературным символом этических аспектов эксплуатации роботов и ИИ стали знаменитые «Три закона робототехники» А. Азимова, впервые сформулированные автором в рассказе «Хоровод» 1942 г.

Сегодня обсуждение этических проблем, связанных с использованием интеллектуальных машин, вышло далеко за пределы научной фантастики и дало необходимую почву для формирования нового исследовательского направления, которое получило название «робоэтика» и стало частью более крупного направления – этики ИИ [1].

В 2004 г. в Италии состоялся Первый Международный симпозиум по робоэтике, после которого в том же году состоялось принятие в Японии Всемирной декларации о роботах. П. Асаро выделяет три составляющие понятия «робоэтика»: встроенные в роботов этические системы; этика людей, которые разрабатывают и используют роботов; этика обращения людей с роботами.

Министерство внутренних дел (МВД) России уже использует информационные системы и программное обеспечение в сочетании с технологией машинного распознавания изображений [3].

Кроме того, эти технологии могут идентифицировать лиц, находящихся в розыске или подозреваемых в совершении преступления, угнанные или подозрительные транспортные средства. Биометрическая система идентификации, разработанная МВД России, позволяет осуществлять поиск с помощью набора информации, содержащей фотографические изображения людей, в том числе: разыскиваемых и пропавших без вести; лиц, содержащихся в информационной системе МВД России.

Следует отметить, что в настоящее время разрабатывается программное обеспечение, которое позволит выявлять перспективные преступления из числа нераскрытых преступлений последних лет с целью их раскрытия. Этот механизм достигается путем создания прогностической модели для выявления преступности на основе наиболее важной информации, содержащейся в статистической таблице.

В качестве инструмента используется открытая библиотека ИИ, разработанная отечественными ИТ-компаниями. Еще одним важным направлением является развитие робототехники, в том числе систем управления наземными и воздушными роботизированными комплексами, а также возможностей беспилотных летательных аппаратов.

МВД России придает большое значение использованию беспилотных летательных аппаратов для поддержки деятельности органов внутренних дел по охране общественного порядка, обеспечению общественной безопасности, борьбе с преступностью, противодействию коррупции, экстремизму и терроризму.

Например, принцип их работы заключается в следующем. Система состоит из двух нейронных сетей. Первый обрабатывает поток изображений с камеры и определяет, есть ли там лицо. Она «вырезает» и «выравнивает» каждого из них. Современные нейронные сети могут просматривать 1 млрд изображений из базы данных менее чем за полсекунды с точностью почти до 100 %.

Второй набор сценариев, использующих системы ИИ, является более обыденным и фактически отражает автоматическое заполнение программных документов на основе содержимого ранее проанализированных документов.

В этом случае могут использоваться системы автозаполнения времени и места (для протоколов), исправления ошибок и стилистических неточностей, транскрибирование устной речи участников следственных действий. В этом случае задачи классификации и прогнозирования ИИ могут быть выполнены. Использование этих систем может предоставить исследователям более точные данные, тем самым повышая скорость и качество принятия решений.

Так, в некоторых частях Китая нашли потенциальных преступников с помощью ИИ до того, как они нарушили закон. Камеры с системами распознавания лиц следят за гражданами и сообщают правоохранительным органам, если в объектив попадает что-то подозрительное.

Например, если кто-то покупает слишком много удобрений за один раз – в конце концов, их можно использовать для подготовки к террористическим атакам. Человека, уличенного в сомнительном поведении, полиция имеет право арестовать или направить на принудительное перевоспитание.

В других странах также пытаются предсказать преступления. В некоторых регионах Соединенных Штатов Америки и Соединенного Королевства Великобритании и Северной Ирландии полиция использует компьютерные системы для определения места возможных инцидентов в ближайшем будущем. Они учитывают множество факторов: криминальную историю региона, его социально-экономический статус и даже прогноз погоды. Удивительно, но с появлением «Оракула» количество перестрелок в районе Чикаго, где он работал, сократилось примерно на треть.

Быстрое развитие и применение новых технологий требует тщательного контроля, особенно в вопросе ответственности. Виновен или не виновен, вот в чем вопрос. В будущем ИИ будет использоваться не только для решения текущих проблем, но и во всем мире, что может существенно повлиять на будущее человечества.

Очевидно, что по мере развития и расширения доступности технологий умного города, датчиков и Интернета вещей ИИ и машинное обучение будут по-прежнему внедряться в правоприменительную практику. Конечно, возможности систем ИИ не ограничиваются этим списком. Такая технология обладает большим потенциалом, в том числе для решения частных и общих задач правоохранительных органов.

Список использованных источников

1. Введенская, Е.В. Актуальные проблемы робоэтики / Е.В. Введенская // Науковедч. исслед. – 2019. – С. 88–101.

2. Караваева, А.В. Некоторые вопросы использования современных технологий в правоохранительной деятельности и предупреждении преступлений / А.В. Караваева // Вестн. Алт. акад. экономики и права. – 2021. – № 5–1. – С. 135–141.

3. Малина, М.А. Цифровизация российского уголовного процесса: искусственный интеллект для следователя или вместо следователя / М.А. Малина // Рос. следователь. – 2021. – № 2. – С. 29–32.

4. Рыжкова, Е.А. Искусственный интеллект как элемент цифрового отношения / Е.А. Рыжкова, Е.К. Рыжкова // Юрид. исслед. – 2022. – № 8. – С. 1–11.

5. Юдина, М.А. Индустрия 4.0: перспективы и вызовы для общества / М.А. Юдина // Гос. упр. Электрон. вестн. – 2017. – № 60. – С. 197–215.

УДК 343.985

С.А. Корнеев, Э.А. Лопатьевская

КИБЕРПРЕСТУПНОСТЬ И НЕКОТОРЫЕ ВОПРОСЫ ПОДГОТОВКИ ЮРИСТОВ

Одной из новых форм транснациональной преступности является киберпреступность. Когда речь заходит о «киберпреступлении» используются разные понятия – «преступление в сфере компьютерной информации», «преступление в сфере высоких технологий» и др. Чаще всего совершаются преступления, связанные с неправомерным использованием персональных данных.

Согласно ст. 1 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано; предоставление персональных данных – действия, направленные на ознакомление с персональными данными определенных лица или круга лиц; распространение персональных данных – действия, направленные на ознакомление с персональными данными неопределенного круга лиц; субъект персональных данных – физическое лицо, в отношении которого осуществляется обработка персональных данных.

Интернет стал средством обмена информацией по всему миру. Размещая в сети Интернет свою персональную информацию, гражданин может создать условия для совершения в отношении себя киберпреступлений.

Уголовная ответственность за киберпреступления предусмотрена в ряде статей Уголовного кодекса Республики Беларусь: ст. 212 «Хищение имущества путем модификации компьютерной информации»; ст. 349 «Несанкционированный доступ к компьютерной информации»; ст. 350 «Уничтожение, блокирование или модификация компьютерной информации»; ст. 352 «Неправомерное завладение компьютерной информацией»; ст. 354 «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств»; ст. 355 «Нарушение правил эксплуатации компьютерной системы или сети».

В соответствии со ст. 1 Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации; информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Активное использование информационных технологий почти во всех сферах жизнедеятельности предполагает повышение требований к подготовке юристов.

По нашему мнению, в системе подготовки юридических кадров, наряду с необходимостью изучения требований по обеспечению надежности защиты информации на основе технических и программных средств, должны рассматриваться и правовые нормы, направленные на сохранность ведомственной информации и противодействие киберпреступности.

Следовательно, учебный анализ правовых норм должен предшествовать изучению методов по защите информации на основе технических средств и систем и противодействию киберпреступности.

Одним из направлений подготовки специалистов – юристов является включение в учебные программы вопросов по противодействию киберпреступлениям, предусматривающих не только теоретическую, но и практическую подготовку. Отдельные вопросы по противодействию киберпреступности можно включать в программу преддипломной практики.

Считаем также целесообразным вопросы по противодействию киберпреступности предусматривать в программах научно-практических конференций, приводимых на юридических факультетах с участием специалистов в данной сфере.

В заключение отметим, что в современных условиях важен системный, комплексный подход при подготовке специалистов, обладающих навыками по обеспечению сохранности ведомственной информации и противодействию киберпреступности.

УДК 393.985

В.В. Кравец

ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ

Стремительное развитие информационных технологий, их широкая доступность и мгновенная возможность обмена информацией в сети Интернет, преобразует интернет-пространство в мощное оружие, целью которого является воздействие на сознание людей.