несмотря на сверхмощную скорость обработки информации, в разы превосходящую возможности человека, ИИ остается программой с привязанным к ней материально-техническим обеспечением. Ответственность за деятельность, связанную с применением ИИ, должны нести лица, использующие ИИ как объект повышенной опасности.

А.В. Макутчев, прогнозируя возможности и пределы внедрения ИИ в правоохранительную деятельность, выделяет три эволюционных этапа информатизации: трансформация всех процессов путем углубленного внедрения цифровой обработки данных; использование систем ИИ без непосредственного их участия в принятии решений; углубленное внедрение, когда система ИИ в той или иной степени заменяет собой сотрудников.

Очевидно, что внедрение систем ИИ в правоохранительную деятельность должно сопровождаться административными и организационными мерами. Однако основанием для наказания граждан могут быть только официальные юридические решения и документы.

УДК 378.6:004.45

И.С. Ивануха

ПОДГОТОВКА КАДРОВ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Активный рост киберпреступлений, совершенных с использованием информационно-телекоммуникационных технологий, наблюдаемый на территории России, так и во всем мире, порождает потребность в увеличении численности сотрудников органов внутренних дел (ОВД), способных эффективно решать задачи по предотвращению, выявлению, раскрытию и расследованию киберпреступлений с использованием и применением информационных технологий.

Киберпреступления в сфере компьютерной информации относятся к числу наиболее распространенных на сегодня видов преступлений. Следует отметить также, что методы совершения данных преступлений постоянно совершенствуются. Соответственно, вопрос противодействия и привлечения к уголовной ответственности лиц за совершение указанных противоправных деяний является весьма актуальным. Несмотря на широкое распространение преступлений в сфере компьютерной информации, на данный момент нет четкого определения в Уголовном кодексе Российской Федерации понятий «киберпреступность» и «киберпреступление».

Соответственно, вопросы противодействия и привлечения к уголовной ответственности лиц за совершение киберпреступлений являются весьма актуальными и нуждаются в подробной регламентации. При этом, несмотря на уменьшение зарегистрированных преступлений с использованием современных информационно-коммуникационных технологий, официальная статистика [1] не отражает объективную картину распространения киберпреступлений, показывая лишь незначительную часть реально совершенных. Происходит это из-за отсутствия единообразия в национальном уголовном законодательстве стран СНГ и негативно отражается на развитии методов эффективной борьбы с киберпреступностью – явлением, для которого не существует государственных границ. Наличие глобальных информационных сетей стирает границы информационного пространства, а «виртуальные» границы между государствами легко пересекаются киберпреступниками, орудующими в любом месте киберпространства, независимо от юрисдикции государств, с помощью компьютера и доступа в сеть Интернет. Отражается это и на эффективности международного сотрудничества в борьбе с киберпреступностью, которое невозможно, если в законодательстве одной страны деяние считается преступлением, а в другой – уголовной ответственности не предусмотрено.

По данным правоохранительных органов, только за последний год распространенность преступлений различных видов, совершаемых с использованием информационных технологий, значительно увеличилась. Результаты анализа, проведенного Организационно-аналитическим департаментом МВД России, указывают на то, что количество зарегистрированных преступлений данной категории за девять месяцев 2022 г. и аналогичный период прошлого года снизилось на 4 %. При этом отношение числа раскрытых преступлений к общему числу преступных деяний, так называемая раскрываемость преступлений составила всего 30 %. Следует обратить внимание на то, что раскрываемость преступлений рассматриваемой категории весьма низкая.

Данная ситуация обусловлена тем, что сотрудники ОВД при расследовании таких преступлений допускают ошибки, которые в большинстве своем являются следствием их низкой профессиональной подготовки именно для раскрытия киберпосягательств. Например, минимальными знаниями по специальности «Информатика и вычислительная техника» обладают только 3,5 % сотрудников [5]. Стоит отметить, что невозможно эффективно предотвратить, выявить, раскрыть и расследовать киберпреступления без использования и применения информационных технологий.

К сожалению, существующая в нашей стране система противодействия преступлениям, которые совершаются с использованием современных технологий, в своем развитии еще заметно отстает [2]. Одна из основных причин низкой раскрываемости киберпреступлений – это низкая квалификация сотрудников ОВД во многих подразделениях. На наш взгляд, эта сложность обусловлена тем, что, несмотря на относительную дешевизну и повсеместную распространенность компьютеров, они недоступны для всех слоев населения. Считаем, что проблема кроется глубже, в школах недостаточное внимание уделяется дисциплине «Информатика и вычислительная техника». Поступая в высшее учебное заведение, многие впервые взаимодействуют с компьютером и впервые начинают получать базовые знания. Несмотря на то что в учебных заведениях МВД России и в рамках межведомственного взаимодействия с гражданскими вузами проводится повышение квалификации действующих сотрудников, специализирующихся на противодействии киберпреступлениям. Это не решает проблему в целом из-за недостаточной динамичности и гибкости системы образования в формировании компетентности специалистов юридического профиля к деятельности по противодействию киберпреступлениям [3]. Имеет место быть также низкое технологическое и программное оснащение образовательных организаций.

Вторая немаловажная причина – это отсутствие надлежащей подготовки и технологического оснащения действующих подразделений ОВД, которые непосредственно занимаются раскрытием киберпреступлений.

Например, по словам Саги Бар – генерального директора центра киберобразования в Израиле, в школах дети уже с первого класса учатся читать, писать и кодировать. В стране даже есть детские сады, где учат работе на компьютере и робототехнике. С четвертого класса ученики уже активно изучают программирование, а одаренные старшеклассники – технологии шифрования и методы борьбы с «черным хакерством» [4]. О том, насколько глубоки знания израильских школьников, можно судить по их развлечениям. Дети играют в игры, по условиям которых, например, взломана воображаемая компьютерная сеть, и у ребят есть 45 минут, чтобы узнать неизвестный компьютерный код, восстановить контроль за сетью и взломать систему злоумышленника, чтобы установить его личность.

В результате проведенного нами исследования, считаем, на современном этапе целесообразным сочетание подготовки соответствующих специалистов юридического профиля, а также одновременного повышения уровня базовой информационно-технической подготовки всех сотрудников ОВД. Определить специальные компетенции, которыми

должны обладать сотрудники ОВД, осуществляющие противодействие киберпреступности.

Считаем, что сотрудник должен обладать навыками и знаниями в области информационных технологий и кибербезопасности: архитектуры и организацией функционирования электронно-вычислительных машин; современных вычислительных систем и сетевых технологий; современных операционных систем; работы с большими данными; системы искусственного интеллекта; мониторинга информационных сетей; уязвимости современного программного и аппаратно-программного обеспечения; общих методов и средств обеспечения кибербезопасности; защищенных сетевых технологий глобального и локального назначения; функционирования электронных платежных систем. Понимание технологий реализации угроз кибербезопасности: атаки на информационные ресурсы, атаки на компьютерные сети, атаки на электронные платежные системы; поиск следов преступной деятельности и методика выявления (раскрытия) киберпреступлений. В области подготовки специалистов в данной сфере целесообразно определить направления работы по обеспечению образовательного процесса [5]: организация взаимодействия ОВД и участие в разработке учебных программ, организация работы филиалов кафедр, проведение совместных занятий, проведение стажировки, практики; совершенствование образовательного процесса с учетом изменяющихся подходов и перспектив в сфере противодействия киберпреступности; повышение уровня подготовки профессорско-преподавательского состава, организация повышения квалификации по данному профилю, стажировка в практических подразделениях ОВД, участие в тренингах, семинарах, конференциях; внедрение компьютерных технологий в образовательный процесс, применение в образовательном процессе специализированного программного и программно-аппаратного обеспечения, используемого в раскрытии киберпреступлений; создание практико-ориентированной среды в образовательном процессе; активизация научно-исследовательской работы по проблемам противодействия киберпреступности.

Список использованных источников

1. ЦСИ ФКУ ГИАЦ МВД России [Электронный ресурс]. – Режим доступа: http://10.5.0.16/csi/modules.php?name=Books&go=check&id=280. – Дата доступа: 25.10.2022.

2. Шевченко, Е.С. Актуальные проблемы расследования киберпреступлений / Е.С. Шевченко // Эксперт-криминалист. – 2015. – № 3. – 169 с.

3. Чукова, Д.И. Проблемы подготовки специалистов по расследованию компьютерных преступлений / Д.И. Чукова // Лучшая научно-исследовательская работа 2019 : сб. ст. – Уфа : ООО «Науч.-изд. центр «Вестн. науки», 2019. – С. 103–108.

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].