Таким образом, одним из подходов к решению обозначенной проблемы может быть выбор иерархического метода классификации социальных групп и последовательного распределения социальных групп на подчиненные классификационные объекты. Глубина классификации определяет количество уровней классификации, а ширина – число классификационных признаков. К достоинствам такой иерархической системы классификации можно отнести простоту построения и восприятия, возможность использования независимых классификационных признаков в различных ветвях иерархической структуры.

УДК 34. 047

А.В. Ивановский, Д.Д. Пашкевич

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

В условиях геополитического транзита все большую роль в развитии права начинают играть национальные интересы, государственное управление, активность социальных групп общества, информационные технологии, правовой опыт. Необходимость обработки интенсивно возрастающих потоков информации ведет к развитию новых организационно-правовых форм и методов ее обработки.

К одному из подходов к автоматизации процессов управления относят технологии искусственного интеллекта (ИИ). При этом в зависимости от степени зрелости конкретной технологии выделяют направление ее использования при принятии решений:

вспомогательное средство для выбора наилучшей альтернативы для решения; консолидации отчетности; предоставления данных управленцам в режиме реального времени;

разработка сценариев развития ситуации с применением когнитивных методов, прогнозирование последствий принятия решений;

выполнение функций управления, требующих больших объемов вычислений перед принятием решений. При этом люди используют полученные с помощью ИИ результаты в качестве основы для окончательного принятия решений;

высказывание самостоятельного мнения с помощью ИИ по проблемам, требующим решений;

выполнение функций верхнего уровня управления. Например, разработку стратегии, назначение на должности и т. п.

С учетом этого применения идей и технологий ИИ носит дискуссионный характер, связанный «с усложнением информационных отношений, при котором появляются новые информационные ценности и, как следствие, новые формы общественно опасных посягательств на них».

Под системой в ЕС ИИ понимается «система, которая:

принимает данные машинного и (или) человеческого происхождения и входные сигналы;

делает логические выводы о том, как достичь набора целей, определенных человеком, используя обучение, рассуждение или моделирование, которые реализуются посредством указанных ниже методов;

генерирует результаты в виде контента (генеративные системы ИИ), прогнозов, рекомендаций или решений, которые влияют на среду, с которой система взаимодействует».

К числу методов относят подходы, применяемые при разработке систем ИИ:

машинное обучение, включающее обучение с учителем, без учителя, обучение с подкреплением, с применением широкого спектра различных методов, включая глубокое обучение;

подходы, основанные на логике и на инженерии данных, включая представление знаний, индуктивное (логическое) программирование, базы знаний, механизмы вывода и дедукции, (символьное) формирование рассуждений и экспертные системы;

статистические подходы, байесовское оценивание, методы поиска и оптимизации.

А.А. Васильев, Ю.В. Печатнова отмечают, что ИИ нельзя считать классическим объектом правового регулирования, но и нельзя рассматривать как полноценный субъект права по следующим причинам:

традиционная концепция о субъектах права исходит из того, что участниками правоотношений являются физические и юридические лица;

попытки сравнения ИИ с физическими лицами не выдерживают критики с точки зрения физиологии;

когнитивные способности ИИ весьма ограничены в сравнении с человеческими функциями мозга.

Искусственная нейронная сеть, построенная по принципу функционирования нервных клеток живого организма, значительно уступает строению биологической нейронной сети по количеству слоев нейронов, кроме того в человеческом мозге обмен информацией между нейронами идет не последовательно, а параллельно и асинхронно.

Исследователи проблемы ИИ фокусируют внимание на правовой необоснованности признания ИИ субъектом права ввиду того, что ИИ не является носителем критически важных составляющих личности (души, свободного сознания, чувств, устремлений, личных интересов). Поэтому,

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.