Для обеспечения эффективной защиты информации необходимо постоянно следить за новыми разработками и внедрять комплексные решения, включающие как традиционные, так и инновационные технологии.

Важно отметить, что обеспечение информационной безопасности в УИС является большим шагом к укреплению безопасности системы в целом. Внедрение современных технологий защиты информации, таких как системы обнаружения вторжений, шифрование и управление доступом, будет способствовать созданию надежной и устойчивой к угрозам среды, обеспечивающей не только сохранность данных, но и бесперебойную работу УИС, как целостной системы.

УДК 351.74

Ю.А. Сурженко, Я.В. Крупский

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ДЕЯТЕЛЬНОСТИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПО ОБЕСПЕЧЕНИЮ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Обеспечение общественной безопасности является актуальным направлением для всех развитых стран мира. В данной сфере различными организациями проводится постоянный мониторинг с опубликованием рейтингов, результаты которых имеют существенное влияние при выборе места проживания, привлечения туристов, инвесторов и др. На помощь правоохранительным органам приходит стремительно развивающийся искусственный интеллект (далее – ИИ), который уже успел стать частью жизни многих людей.

Целесообразно рассмотреть способствование ИИ правоохранительным органам Республики Беларусь и других стран в обеспечении общественной безопасности.

Для того, чтобы понять, как он может помочь, необходимо определить, где правоохранительным органам нужна помощь.

Первой проблемой являются дипфейки, создаваемые ИИ. Дипфейк (англ. deepfake) – методика синтеза изображения или голоса, основанная на ИИ. В 2024 г. ИИ так сильно развился, что сейчас человеческому глазу становится все сложнее и сложнее отличить, где реальность, а где дипфейк. С помощью дипфейков можно распространять фейковые новости, например, о руководстве МВД, Главе государства и т. д., что может привести к массовому недовольству или перерасти во что-то большее. Дипфейк используется для шантажа людей, которые, опасаясь за свою

репутацию, слепо следуют указаниям мошенников. Для противодействия дипфейкам целесообразно начать обучать его распознанию (что является реальностью, а что дипфейком). ИИ является более умным, чем человек, способен заметить различные мелочи, а если начать его обучать в узком направлении, то, вероятнее всего, ИИ начнет помогать бороться с проблемой дипфейков.

Второй проблемой является сложность поиска лиц по Республиканской системе мониторинга общественной безопасности (далее – РСМОБ). В настоящее время для поиска людей через РСМОБ нужно иметь достаточно четкую фотографию и нужный ракурс, так как процент совпадения с некачественной фотографией очень низок. В данном случае ИИ можно обучить самостоятельно улучшать качество фотографии, распознавать лица, даже если фото было сделано с неудачного ракурса. В настоящий момент существуют различные платные и бесплатные сервисы по улучшению качества фотографий, а также поиску лиц по фото. В этой связи просто улучшить эти функции не должно составить большого труда, однако отсюда вытекает проблема процессуального регулирования. Например, судья при вынесении решения не может быть уверен, что ИИ, улучшив качество фотографии, не исказил изображение лица и выдал именно то лицо, которое должно быть привлечено к ответственности.

Третьим вариантом применения ИИ может стать анализ видеонаблюдения, который поможет не только сотрудникам правоохранительных органов, но и органам безопасности аэропортов, магазинов и пр. Все мы знаем понятие «профайлинг», которое впервые использовалось службой авиационной безопасности в аэропорту Бен-Гурион в Израиле для выявления террористов. Данный метод помогал выявлять необычное поведение людей, которых в кротчайшие сроки задерживали, благодаря чему было предотвращено множество терактов. Обучение ИИ при помощи специальных видеороликов и видеозаписей, на которых задерживали настоящих террористов, позволит увеличить скорость и точность распознавания возможной угрозы. Это можно применить и в вышеупомянутой РСМОБ. С помощью повсеместно установленных камер видеонаблюдения, можно выявить преступников по различным признакам, например: слишком часто оборачивается; избегает встречи с сотрудниками милиции; пытается что-то скрыть внутри одежды будто что-то украл, пытается что-то незаметно выбросить. Это поможет как раскрывать, так и пресекать различные правонарушения.

ИИ можно применить в автоматизации рутинных задач, например, оформление процессуальных документов. Иногда сотрудники не успевают составить нужное количество документов для передачи материа-

лов в Следственный Комитет, что влечет за собой нарушение процессуальных сроков. В таком случае можно внедрить ИИ в программу, которая автоматически оформит документ, если предварительно внести туда ключевые данные, например, ФИО обвиняемого, квалификация и т. д.

Однако проблемами внедрения ИИ в деятельность правоохранительных органов является финансирование и нехватка специалистов в данной сфере. В настоящее время для обучения ИИ нужно потратить большое количество средств только для создания нужной среды (закупка мощных компьютеров, постройка или аренда помещения для их размещения). Этот аспект следует учитывать, потому как обучение ИИ происходит на одновременном проигрывании множества сценариев в течении большого количества времени. В свою очередь обучать ИИ рядовой пользователь компьютера не сможет, для этого необходимо не только хорошее владение языком программирования, но и прохождение дополнительных курсов по обучению ИИ.