УДК 343.985.7; 004.048

Н.А. Кузьмин

ОБ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРОТИВОДЕЙСТВИИ КОРРУПЦИОННЫМ ПРЕСТУПЛЕНИЯМ

В настоящее время современное развитие науки и техники неминуемо влечет за собой изменение средств и методов борьбы с преступностью. Не является исключением в этой связи совершенствование вопросов противодействия коррупционным преступлениям, которые продолжают оставаться серьезной угрозой для поступательного развития России.

Эволюция системы искусственного интеллекта в разнообразных сферах деятельности нашей страны показывает возрастающую ее актуальность, эффективность и, как следствие, востребованность для использования органами внутренних дел в противодействии преступности.

В Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. № 490, под искусственным интеллектом понимается комплекс технологических решений, позволяющий имитировать когниктивные 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.

В книге «Искусственный интеллект. Большие данные» В.С. Овчинский и Е.С. Ларина определяют искусственный интеллект как вычислительную платформу для выполнения конкретных, заранее заданных функций и решения задач, устройство превращения любой (визуальной, акустической, текстовой и т. п.) информации в цифру, обработка этой цифры методами статистики и дискретной вычислительной математики и получение ответа в интуитивно понятном для человека виде. Именно искусственный интеллект является основой для сбора, хранения и обработки информации.

На фоне продолжающегося распространения коррупционных преступлений искусственный интеллект становится действенным инструментарием для противодействия деятельности нечистых на руку чиновников. Это в первую очередь обусловлено тем, что искусственный интеллект невозможно подкупить, скрыть выявленное коррупционное правонарушение или убедить его в чем-либо. Принимаемые им решения обусловлены конкретными алгоритмами, которые тяжело изменить или перенастроить. Сегодня программы, работающие с использованием искусственного интеллекта, позволяют не только определять по подозрительной банковской активности потенциальную взятку, но и прогнозировать развитие коррупции задолго до ее появления. Искусственный интеллект также помогает найти в различного рода документации, прежде всего финансового, бухгалтерского характера, сведения, свидетельствующие о причастности отдельных лиц к совершению коррупционных преступлений, либо иную информацию, указывающую на коррупционные факты, а также противоправные действия чиновников.

Подобные системы уже показали свою эффективность в других странах. Особенно ценен опыт Китая в этом направлении. Развернутая в пилотном варианте система искусственного интеллекта Zero Trust позволила выявить тысячи коррупционеров и получить конкретные доказательства их преступной деятельности.

Работа данной системы была построена на основе сопоставления множества баз данных федерального и регионального уровней с доходами и расходами государственных служащих. Это позволило с высокой долей эффективности выявлять наиболее характерные и распространенные коррупционные правонарушения, связанные с незаконной передачей прав собственности на имущество, со злоупотреблениями в сфере земельных отношений, махинациями при проведении различного рода тендеров и т. д. Безусловно, что при обработке большого количества различных данных система искусственного интеллекта Zero Trust не могла однозначно указывать на совершение коррупционного преступления или правонарушения и решающий вывод был за оператором. В этой связи можно сделать вывод о том, что искусственный интеллект, обрабатывая большие объемы данных, дает возможность оператору сосредоточиться на важных, имеющих значение деталях, свидетельствующих о наличии или отсутствии признаков коррупционных преступлений.

Несмотря на высокую эффективность подобных программ для борьбы с коррупцией, их использование вызывает ряд вопросов. Так, очевидно, что для определения фактов коррупции, в основе которых лежит сопоставление сведений о доходах и расходах чиновников и информации, содержащейся в различных базах данных, искусственному интеллекту потребуется анализировать информацию, находящуюся не только в государственных органах, но и в других организациях, в том числе в банках. В этой связи неминуемо возникают вопросы правового характера. Так, согласно ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Закономерно встает вопрос о доступе системы искусственного интеллекта к данным таких организаций без каких-либо ограничений. Этот вопрос представляется чрезвычайно важным, поскольку сегодня продолжаются тенденции уменьшения доли наличных денежных средств при каких-либо действиях коррупционеров по легализации преступно нажитых денежных средств (операциях по купле-продаже товаров и услуг, недвижимости и т. д.). Системы отслеживания транзакций интересующих фигурантов, ввода и вывода денежных средств при помощи искусственного интеллекта могут охватить практически все траты конкретного лица. И если раньше такие мероприятия требовали использования значительных ресурсов для проверки сведений о доходах и расходах чиновников путем направления запросов в различные ведомства, то теперь искусственный интеллект может существенно сократить время проведения таких проверок. В результате чего для анализа оператору будут попадать совершенно конкретные факты, свидетельствующие, например, о том, что чиновник совершает траты значительного количества денежных средств, их переводы либо получает на свой счет необоснованные суммы денег и т. д.

Бесспорно, что при создании подобной системы искусственного интеллекта в России органы внутренних дел смогут получить дополнительный инструментарий для противодействия коррупционным преступлениям, что позволит своевременно

реагировать на имеющуюся информацию и предпринимать необходимые меры. Следует отметить, что для реализации подобных предложений в России уже проделана значительная работа. Сегодня удалось сформировать основные контуры сотрудничества компаний в финансовой сфере. Например, платформа обмена данными о киберугрозах, реализованная под эгидой Ассоциации банков России, в настоящее время объединяет порядка 70 финансовых организаций, включая крупнейшие финансовые институты страны. Полагаем, что использование данных платформ при создании системы искусственного интеллекта позволит в кратчайшие сроки объединить имеющиеся ресурсы для противодействия коррупционным преступлениям.

УДК 343.98

Д.Н. Лузько

ИМИТАЦИЯ ПРЕСТУПНОГО ПОВЕДЕНИЯ В ХОДЕ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ: ПРАВОВЫЕ И ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ

Современная преступность, обладая высокой степенью латентности, меняет не только свои количественные, но и качественные характеристики. При этом лица, совершающие преступления, часто осведомлены о средствах и методах, применяемых правоохранительными органами для борьбы с криминальными проявлениями. В связи с чем оказывают им целенаправленное противодействие, принимая меры к сокрытию следов преступлений и защите от разоблачения. Именно поэтому одним из первостепенных и активных средств государственного противоборства с преступностью выступает оперативно-розыскная деятельность, основой которой является ее осуществление посредством проведения оперативно-розыскных мероприятий.

Несмотря на то что в Федеральном законе Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон об ОРД) список указанных мероприятий конкретизирован, нам импонирует точка зрения Н.С. Железняка, отмечающего, что «ОРМ хотя и выступают стержневым элементом ОРД, но не являются ее единственными составными частями». Действительно, исходя из оперативно-розыскной практики, помимо зафиксированных в Законе об ОРД мероприятий оперативным сотрудникам приходится осуществлять множество иных действий (в том числе их совокупность), структурно не входящих в ОРМ, либо частично пересекающихся с ними, но не менее важных для решения задач противодействия преступности. Данный дисбаланс, по выражению А.Е. Чечетина, «сковывает инициативу оперативных работников, их творческий подход к решению задач борьбы с наиболее опасными видами преступлений». Последнее, в свою очередь, препятствует развитию оперативно-розыскной тактики, внедрению новых, не предусмотренных законом, но основанных на достижениях науки и техники форм и методов ОРД. Одной из таких мер, позволяющих обеспечить высокий уровень конспирации при проведении мероприятий по противоборству преступным проявлениям, проникновению в криминальную среду (здесь и далее мы подразумеваем оперативное внедрение в преступные группы, сообщества и на объекты оперативной заинтересованности), выведыванию ее намерений и планов, пресечению противоправной деятельности ее субъектов является имитация преступного поведения. Данное мероприятие, формально не закрепленное в российском оперативно-розыскном законодательстве, нередко является ее неотъемлемой частью и используется при реализации частных и общих задач ОРД.

Для того чтобы определить значение имитации преступного поведения в ОРД, кратко рассмотрим ее суть. Как у всякого сложного многоаспектного явления, у имитации не существует единой канонической дефиниции. Термин «имитация», происшедший от латинского imitatio, означает подражание и в своем широком философском понимании представляет собой создание формы по образу совершенного. В толковых и энциклопедических словарях она, как правило, определяется как искусное подражание кому-либо, чему-либо, воспроизведение чего-либо с возможной точностью, создание образа, модели объекта или процесса, его искусственное воспроизведение.

Применительно к ОРД имитация может использоваться в различных оперативно-тактических комбинациях. Например, в ходе проведения легендированого, с зашифровкой цели ОРМ «опрос» среди лиц криминальной направленности, субъект ОРД (оперативный сотрудник или лицо, ему содействующее) с целью получения оперативно значимой информации может применить элементы имитации преступного поведения, выраженные в показательной причастности к криминальной среде (сленговый или жаргонный разговор, татуировки; сопутствующие криминальному образу различные атрибуты, манера поведения и т. д.).

При проведении ОРМ «оперативный эксперимент» субъект ОРД негласно моделирует и воспроизводит контролируемые искусственные условия, погружая в них объект разработки, для последующего документирования его преступных действий. Ярким примером осуществления указанного мероприятия служит пресечение заказных убийств, в ходе которого имитируется факт совершения преступления, и заказчику предоставляются материалы, подтверждающие совершение «фиктивного убийства».

Наиболее выраженно имитация преступного поведения проявляется при оперативно-тактических комбинациях, способствующих оперативному внедрению субъекта ОРД в криминальную среду и при обеспечении последующего его нахождения в ней. В таких случаях от субъекта ОРД требуется максимум его способностей и профессиональных качеств, предполагающих необходимость осуществить перевоплощение и вжиться в роль преступника. В связи с этим, не вдаваясь в организационные и тактические особенности внедрения, целесообразно описать личностные факторы субъекта ОРД, использующего имитацию преступного поведения, влияющие на успешное проникновение в криминальную среду:

1) психолого-коммуникативный фактор, т. е. психологическую готовность субъекта ОРД, его профессиональное мастерство, необходимое для эффективного применения сил, средств и методов ОРД при подготовке и проведении ОРМ, направ-