Organization for Security and Co-operation in Europe
Programme Office in Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ЖОҒАРҒЫ СОТЫ

«СОТ ЖӘНЕ ҚҰҚЫҚ ҚОРҒАУ ЖҮЙЕСІНДЕГІ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ ҮЛКЕН ДЕРЕКТЕР (BIG DATA): ШЫНДЫҚ ЖӘНЕ УАҚЫТ ТАЛАБЫ»

Халықаралық ғылыми-практикалық конференциясы
МАТЕРИАЛДАРЫ

МАТЕРИАЛЫ
Международной научно-практической конференции

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И БОЛЬШИЕ ДАННЫЕ (BIG DATA) В СУДЕБНОЙ И ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЕ: РЕАЛИИ И ТРЕБОВАНИЕ ВРЕМЕНИ»

THE MATERIALS
of the International scientific and practical conference

«ARTIFICIAL INTELLIGENCE AND BIG DATA IN THE JUDICIARY AND LAW ENFORCEMENT: REALITIES AND NEEDS»

АСТАНА, 2023

УДК 004:340
ББК 32.973:67
С69

С69 **«СОТ ЖӘНЕ ҚҰҚЫҚ ҚОРҒАУ ЖҮЙЕСІНДЕГІ ЖАСАНДЫ ИНТЕЛЛЕКТ ЖӘНЕ ҮЛКЕН ДЕРЕКТЕР (BIG DATA): ШЫНДЫҚ ЖӘНЕ УАҚЫТ ТАЛАБЫ»** Халықаралық ғылыми-тәжірибелік конференция материалдары. – Материалы Международной научно-практической конференции **«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И БОЛЬШИЕ ДАННЫЕ (BIG DATA) В СУДЕБНОЙ И ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЕ: РЕАЛИИ И ТРЕБОВАНИЕ ВРЕМЕНИ»** - The materials of the International Scientific and Practical Conference **«ARTIFICIAL INTELLIGENCE AND BIG DATA IN THE JUDICIARY AND LAW ENFORCEMENT: REALITIES AND NEEDS»**. – Қосшы: «Қазақстан Республикасының Бас прокуратурасы жанындағы Құқық қорғау органдары академиясы», 2023. – 350 бет. – Kosshi: Law Enforcement Academy Under The Prosecutor General's Office Of The Republic Of Kazakhstan, 2023. – p.350.

ISBN 978-601-7969-86-8

Жинақ мемлекеттік, құқық қорғау және арнаулы органдарының, отандық және шетелдік ғалымдары, сондай-ақ халықаралық ұйымдардың өкілдері ұсынған сот және құқық қорғау жүйелерінде жасанды интеллект пен үлкен деректерді пайдаланудың озық әдістерінің нәтижелерін қамтиды.

Жинақ материалдары қазіргі заманғы сот және құқық қорғау жүйесіндегі жасанды интеллект және үлкен деректер мәселелерімен айналысатын мамандарға және ізденушілерге арналады.

УДК 004:340
ББК 32.973:67

Баспаға Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының Оқу-әдістемелік кеңесімен ұсынылды.

ISBN 978-601-7969-86-8

МАЗМҰНЫ // СОДЕРЖАНИЕ // CONTENT

КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ СОВРЕМЕННЫХ ВЫЗОВОВ

ҚАЗІРГІ ЗАМАНҒЫ СЫН-ҚАТЕРЛЕР ЖАҒДАЙЫНДАҒЫ КИБЕРҚАУІПСІЗДІК

CYBERSECURITY IN THE CONTEXT OF MODERN CHALLENGES

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СУДЕБНОЙ И ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

СОТ ЖӘНЕ ҚҰҚЫҚ ҚОРҒАУ ҚЫЗМЕТІНДЕ ЖАСАНДЫ ИНТЕЛЛЕКТТІ ҚОЛДАНУ МӘСЕЛЕЛЕРІ МЕН ПЕРСПЕКТИВАЛАРЫ

PROBLEMS AND PROSPECTS OF USING ARTIFICIAL INTELLIGENCE IN JUDICIAL AND LAW ENFORCEMENT ACTIVITIES

Асламбек Мергалиев
Председатель
Верховного Суда
Республики Казахстан

Уважаемые участники и гости конференции!

Разрешите от имени Верховного Суда Республики Казахстан поприветствовать участников Форума.

Хочу выразить особую признательность представителям государственных органов, международных и неправительственных организаций, учебных заведений, принявших приглашения и проявивших интерес к теме конференции.

Быстрое развитие IT-отрасли буквально меняет мир на глазах. От повседневной жизни людей до механизмов реализации государственной политики.

Судебная система – не исключение.

Глава нашего государства постоянно требует развивать электронное правосудие.

Это один основных векторов дальнейшей модернизации судебной системы.

IT-технологии позволяют оперативно и эффективно защищать конституционные права и свободы граждан.

Правосудие становится более доступным и прозрачным для людей и бизнеса.

Вкратце расскажу о состоянии цифровизации правосудия.

Первое. Как вы знаете, пандемия коронавируса внесла свои коррективы в работу судов.

Срочно надо было найти баланс между безопасностью участников процесса и обеспечением доступа к правосудию.

И здесь нашелся определенный плюс - ускорилась цифровизация судебной сферы.

В первые же дни локдауна нарастили IT-мощности во всех судах: установили дополнительные серверы мобильной видеоконференцсвязи, увеличили пропускную способность каналов связи.

Это позволило судам полностью перейти на дистанционный

формат работы.

Хотя сейчас запрета на проведение судебных заседаний в обычном режиме уже нет, онлайн-формат продолжает быть востребованным.

В первую очередь, для сторон, которые экономят и время, и деньги.

Второе. Есть единое электронное окно доступа ко всем судебным услугам. Можно с любого гаджета, из дома через мобильное приложение направить в суд более 100 видов электронных обращений.

Можно удаленно увидеть регистрацию обращения, узнать его статус и в конце получить судебный акт.

Третье. Все залы судебных заседаний оснащены современными системами аудио-, видеофиксации.

IT-сервисы изменили систему взаимодействия людей с судами и позволили двинуться дальше.

Наш новый IT-продукт - «Цифровая судебная аналитика». Он поможет формировать единообразную судебную практику.

В нём впервые применены элементы искусственного интеллекта.

В целом, уровень цифровизации правосудия высоко оценивается не только внутри страны, но и за рубежом.

С получением статуса наблюдателя в Европейской комиссии по эффективности правосудия (СЕПЕЖ) Казахстан участвует в Обзоре о судебных системах государств – членов Совета Европы.

В обзорах Еврокомиссии 2020 и 2022 годов по применению судами IT-технологий Казахстан занимает 4-е место среди 47 стран.

Мы и далее нацелены на упрощение работы судей и удобство получения судебных услуг, поэтому продолжаем активно развивать электронное правосудие.

Утвердили Стратегию цифровизации судебной системы.

Поставили перед собой 3 главные задачи.

Первая. Обеспечить беспрепятственный и удобный доступ к правосудию через IT-сервисы.

Вторая. Автоматизировать судопроизводство и сделать его экономным.

Третья. Начать работать с большими данными, используя передовой мировой опыт.

Увидели много нового в Сингапуре, Объединенных Арабских Эмиратах. Обогатились идеями. Некоторые адаптировали под себя.

Сейчас с интересом смотрим на опыт **Китая** в сфере создания электронных судов. В **Финляндии** - на систему управления уголовными делами. В **Южной Корее** – на автоматизацию рабочих процессов. В **Латвии** – на функционал распознавания речи и преобразования его в текстовый формат.

Уверен, что и сегодня на конференции прозвучит множество интересных инициатив. С удовольствием послушаем.

Искренне желаю всем успехов и плодотворной работы!

Берік Асылов
Генеральный Прокурор Республики Казахстан, государственный советник юстиции 2 класса

Уважаемые участники и гости!

От имени Генеральной прокуратуры Казахстана и от себя лично, горячо приветствую вас по случаю открытия конференции!

Актуальность тематики этого мероприятия повышается с каждым годом.

Информационные технологии становятся драйвером изменений в мире.

Искусственный интеллект широко внедряется в самые разные сферы.

Как справедливо отметил Президент нашей Республики Касым-Жомарт Кемелевич Токаев «Появление нейросетей и искусственного интеллекта привело к подлинно революционным процессам. Уже видны контуры нового жизненного уклада».

Мировой тренд не обошёл стороной и правоохранительную деятельность.

Идти в ногу со временем, от нас требуют два основных фактора.

Во-первых, искусственный интеллект, как и все технологии Четвертой Промышленной революции, открывают новые горизонты для превентивной борьбы с преступностью.

Многие задачи, которые выполняют сотрудники правоохранительных органов – очень трудоёмкие.

Не исключаются риски ошибок и неточностей.

Анализ Больших Данных и автоматизация, позволят, не только ускорить процессы в правоохранительной сфере, но и повысить эффективность профилактики преступности.

Во-вторых, искусственный интеллект открыл широкие перспективы для криминального мира.

В основном это – киберпреступность.

Получает распространение использование роботов-дронов в террористических целях, а также для доставки наркотиков, оружия и других запрещенных предметов.

Это требует принятия адекватных контрмер.

*****

Первые шаги, ведущие к использованию искусственного интеллекта, предпринимают и органы прокуратуры Казахстана.

Активно внедряются АйТи-технологии.

Цифровизация повысила оперативность прокурорского надзора и усилила его правозащитный потенциал.

Прокуроры ежедневно используют смарт-решения в защите прав граждан и бизнеса, а также общественных интересов в уголовной, гражданской и административной сферах.

Это позволило нам избавиться от рутинной работы и в разы повысить её эффективность.

Теперь готовимся к следующему этапу.

Более подробно об этом расскажет на 3-ей секции мой коллега – заместитель председателя Комитета по правовой статистике и специальным учетам – Ерадиль Ахметов.

*****

В то же время, научное сообщество задаётся вопросом об этичности этого процесса.

Высказываются опасения, что использование искусственного интеллекта в правосудии несёт в себе определенные риски.

Поэтому, его внедрение требует прочную научно-практическую основу.

Тут ученым-практикам предстоит большая работа по безопасному внедрению новшеств.

Нужны сценарии реагирования на возможные ошибки и нарушения.

Требуется глубокая ревизия законов.

Возможно, стоит задуматься о введении новых составов правонарушений или квалифицирующих признаков.

Есть вопросы и по уголовному процессу.

Какова допустимость доказательств, собранных и обработанных робот-машиной?

Будут ли иметь юридическую силу такие постановления, приговоры?

В мире уже есть споры на эту тему.

Использование искусственного интеллекта и Больших Данных не должно стать попыткой заменить человека в процессе правосудия.

Главная цель – обеспечить максимальную объективность на основе Больших Данных и сокращение сроков на принятие решений.

При этом мы обязаны позаботиться и о сохранности сведений в базах данных.

Решение этих и других вопросов надо искать и совместно обсуждать на таких площадках.

*****

Уважаемые коллеги!

Благодаря сегодняшней конференции мы имеем возможность обмена мнениями на эту интересную тему.

Желаю всем плодотворной работы и интересных дискуссий.

Благодарю за внимание!

Есқараев Азамат Несіпбайұлы
Қазақстан Республикасының Әділет министрі,
Қазақстан Республикасы, Астана қ.

Уважаемые участники конференции!

Прежде всего, разрешите поприветствовать Вас от имени Министерства юстиции и выразить благодарность организаторам международной научно-практической конференции за приглашение принять в нем участие.

В международных рейтингах Казахстан входит в число наиболее преуспевших в цифровизации государств.

В этой связи, хотел бы отметить, что органы юстиции также вносят посильный вклад в развитие цифрового Правительства.

Так, в части обеспечения исполнения судебных решений на сегодня уже успешно функционирует система АИС ОИП, обеспечивающая прозрачность принимаемых ЧСИ решений, в т.ч. в отношении имущества должников.

Сейчас Министерством юстиции подготовлен пул из 12 проектов Digital Justice охватывающих цифровизацией ключевые направления деятельности Минюста; два из которых - **«E-saraptama» и «E-заң көмегі» - тесно связаны с обеспечением работы правоохранительной и судебной систем.**

Так, система «E-saraptama», предусматривающая повышение качества судебной экспертизы, ее объективности и независимости, позволит автоматизировать взаимодействие как с правоохранительными, так и с судебными органами.

Прозрачность деятельности судебного эксперта будет реализована путем произвольного выбора эксперта автоматизированной системой без участия человека.

В рамках сопровождения планируется модернизировать функционал системы, который позволит усилить ведомственный контроль судебно-экспертной деятельности.

Что касается проекта «E-заң көмегі», то данный проект предназначен для автоматизации деятельности адвокатов, юридических консультантов, их взаимодействия в режиме онлайн с участниками процесса и другими заинтересованными сторонами, в т.ч. в рамках гарантированной государством юридической помощи.

В 2020 году запущен сервис по онлайн процессу назначения адвокатов в рамках ГГЮП «рандомно» в системе электронного уголовного судопроизводства, благодаря чему нивелировались риски выбора «удобного» для дела адвоката.

Также мы планируем реализовать онлайн фиксацию времени, затрачиваемого в рамках ГГЮП для обеспечения справедливой оплаты услуг.

Благодарю за внимание!

Зимин Владимир Петрович
Исполнительный секретарь Координационного совета генеральных прокуроров государств – участников СНГ, государственный советник юстиции 3 класса, Заслуженный юрист Российской Федерации,
г. Москва, Российская Федерация

Уважаемые коллеги!

Позвольте прежде всего от имени Секретариата Координационного совета генеральных прокуроров государств-участников Содружества Независимых Государств (далее – Координационный совет, КСГП СНГ) приветствовать всех участников конференции, а также выразить организаторам конференции признательность за приглашение и возможность высказать ряд соображений по ее тематике.

В повестке дня нашей конференции – серьезные и актуальные вопросы, отражающие одно из наиболее перспективных направлений повышения эффективности как судебной, так и правоохранительной деятельности, а именно: путем использования в ней технологий искусственного интеллекта.

Современные достижения в области искусственного интеллекта создают новые беспрецедентные возможности во многих сферах общественной жизни (прежде всего, в экономике, военном деле, образовании), включая и сферу отправления правосудия. Однако при этом возникают и определенные риски (как явные, так и пока скрытые), в т.ч. криминального характера, и проблемы (в т.ч. связанные с защитой прав человека).

Известно, что многие люди, известные в области информатики, выступили с предупреждением, что бесконтрольное развитие искусственного интеллекта ставит под угрозу само существование человеческой цивилизации потому, что нейросети становятся умнее людей.

Уже сейчас, после довольно непродолжительного периода развития, системы искусственного интеллекта (в первую очередь, ChatGPT) используются в, мягко говоря, неблаговидных целях, в т.ч. для совершения преступлений (например, для взлома компьютеров). Широкие просторы открываются для распространения ложной информации с применением технологии *deepfake,* которая позволяет вполне достоверно изображать человека, совершающего действия, которые он на самом деле никогда не совершал, или говорить какие-то фразы, которые данным человеком никогда не произносились (к примеру, возможно изготовление и распространение порнографической продукции путем подмены в старом порнофильме действующей «героини» изображением другого человека, в т.ч. известного в публичном пространстве (политика, телезвезды, артиста).

Связанные с искусственным интеллектом возможности, риски и проблемы представителям науки и практики предстоит выявить и проанализировать с тем, чтобы создать необходимые и достаточные правовые, организационные и другие предпосылки и условия для создания социально-приемлемых технологий искусственного интеллекта и их надлежащего использования.

В связи с этим Координационный совет и его Секретариат уделяют большое внимание проведению совместного научного исследования в области применения систем искусственного интеллекта в прокурорской деятельности.

Планируется, что в период 2023 –2025 годов под эгидой КСГП СНГ и Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан будет проведено совместное научное исследование по теме «Информационные технологии (искусственный интеллект) в деятельности органов прокуратуры государств – участников СНГ». Намечены и формы завершения исследования. Это монография и практические рекомендации, которые, как мы рассчитываем, найдут свое применение в повседневной прокурорской деятельности.

Итоговые результаты этого исследования будут рассмотрены на заседании Координационного совета.

Очевидно, что наша конференция лежит в русле указанного совместного научного исследования и высказанные на ней мнения

С глубоким удовлетворением хочу отметить тесное взаимодействие Секретариата КСГП СНГ с Академией правоохранительных органов при Генеральной прокуратуре Республики Казахстан на основе двустороннего Соглашения о сотрудничестве от 23 сентября 2021 г., в частности, путем обмена научно-методической и учебно-методической литературой, периодическими изданиями, правовыми актами, актуальными справочными, обзорными, аналитическими материалами и другими документами.

Что касается темы нашей конференции, хотелось бы отметить важность безотлагательного введения жесткой, достаточно детальной и, по возможности, упреждающей правовой регламентации (в т.ч. международно-правовой) вопросов создания и использования искусственного интеллекта, в том числе в правоохранительной деятельности.

В марте т.г. более тысячи ИТ-экспертов, среди которых небезызвестный предприниматель Илон Маск и один из основателей крупной ИТ-корпорации «Apple» Стив Возняк, подписали открытое письмо, призвав не менее, чем на 6 месяцев приостановить работы по созданию и обучению нейросетей, более мощных чем GPT-4, чтобы за это время разработать и внедрить протоколы безопасности, необходимые для обеспечения такой системы контроля и управления в процессе создания и развития технологий искусственного интеллекта,

которая была бы достаточной для безопасного, предсказуемого и транспарентного их применения и развития (на сегодня данное воззвание подписали более 30 тыс. специалистов). Не думаю, что ИТ-сообщество справится с задачей такого саморегулирования (тем более в указанный срок), поскольку гонка с созданием и расширением возможностей систем искусственного интеллекта связана с извлечением огромных прибылей. Поскольку ставка в этом вопросе слишком высока (выживание человечества), основное регулирование должно быть государственным, с применением жестких санкций сдерживающего характера.

Следует активно изучать опыт (причем как положительный, так и отрицательный) зарубежных государств, взявших курс на широкое применение технологий искусственного интеллекта (включая, США, Китай, Германию и Россию), а также заинтересованных международных организаций (в частности, ООН, ЮНЕСКО, СНГ, ОДКБ, Европейского союза, Совета Европы).

Отметим, что Секретариат Координационного совета принимает экспертное участие в нормотворческой работе профильных органов Межпарламентской Ассамблеи государств – участников СНГ (МПА СНГ) и Парламентской Ассамблеи Организации Договора о коллективной безопасности (ПА ОДКБ). В частности, Перспективным планом модельного законотворчества в Содружестве Независимых Государств на 2023 – 2025 годы предусмотрена разработка в 2024 году Модельного закона «О противодействии использованию автономных и роботизированных систем в террористических и экстремистских целях». В рамках ПА ОДКБ идет подготовка Рекомендаций для государств – членов ОДКБ по выработке общих принципов развития национального законодательства в области создания искусственного интеллекта и робототехники в целях обеспечения национальной безопасности.

Полагаю, что при проведении совместного научного исследования в области применения искусственного интеллекта в прокурорской деятельности будут учтены соответствующие наработки МПА СНГ, других профильных органов Содружества (в частности, Антитеррористического центра СНГ и Совета министров внутренних дел СНГ), а также ПА ОДКБ.

Уверен, что для регламентации деятельности, связанной с искусственным интеллектом, необходимо будет также заключать международные договоры на универсальном (прежде всего, под эгидой ООН) и региональном (субрегиональном) уровнях, в том числе в рамках СНГ. Это послужит гармонизации национальных правовых подходов к регламентации деятельности, связанной с искусственным интеллектом, в том числе в сфере установления и реализации ответственности за совершение социально опасных действий. Без такой гармонизации (и даже унификации – применительно к вопросам уголовной

ответственности) невозможным будет правовое сотрудничество государств (например, в вопросах выдачи).

В заключение хочу пожелать всем участникам конференции плодотворной работы, существенного приращения знаний по обсуждаемой тематике и выхода на солидные практические рекомендации, обращенные как к национальным законодателям, так и к практикам.

Благодарю за внимание!

Мусин Бағдат Батырбекұлы
Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрі,
Қазақстан Республикасы, Астана қ.

ЦИФРЛЫҚ ҚҰРАЛДАР-ҚҰҚЫҚТЫҚ ТӘРТІПТІ ҚАМТАМАСЫЗ ЕТУДІҢ ЖАҢА КЕЗЕҢІ

Құрметті қонақтар және әріптестер!

Өздеріңіз білетіндей, бүгінде цифрландыру бойынша үлкен жұмыс атқарылды. Біріккен Ұлттар Ұйымының соңғы зерттеулері бойынша Қазақстан «Электрондық үкіметті дамыту» индексі бойынша **28**-орынға орналасты.

Теперь есть возможность получения государственных услуг и сервисов на смартфонах. Так, в мобильном приложении eGov Mobile можно получить **1 080** видов госуслуг *(за 2022 г. оказано 18,5 млн услуг, за 1 кв. 2023г. оказано 4.7 млн.)*.

Более того, сегодня **16** видов госуслуг можно получить в мобильных приложениях банков второго уровня *(за 2022 г. оказано более 1,08 млн услуг)*. Вывод услуг на внешние платформы необходим для исключения зависимости от единой точки оказания услуг.

Следует отметить, что порядка **40%** заявок на переоформление автотранспорта подаются именно посредством приложений БВУ, что в свою очередь также позволяет снизить количество посещений в СЦОН.

Все это позволило Казахстану занять **8 место в рейтинге ООН** по уровню развития онлайн услуг *(1208 государственных услуг или 92% оказываются в электронном формате)*.

Вместе с тем, мы запустили большую программу цифровой трансформации государственного управления.

Цифровая трансформация – это уже не просто автоматизация процессов, а новый подход, в котором процесс пересматривается через призму технологий.

Соответственно была выработана нормативная, методологическая и экспертная база по цифровой трансформации.

Внедрен реинжиниринг как инструмент оптимизации деятельности госорганов с переводом существующих бизнес-процессов в электронный формат. Сейчас составлен реестр всех функций, с разбивкой их по бизнес-процессам. Госорганами ведется наполнение архитектурного портала для указания в каких системах эти процессы реализуются.

Кроме того, каждый госорган разработал график реинжиниринга функций и процессов. При заинтересованности, приглашаем принять участие в анализе и реинжиниринге - снижение рисков правонарушений основной приоритет.

Например, в АППК внедрена норма, что запрещено запрашивать у граждан и бизнеса те сведения, которые уже есть в информационных системах. Но пока нет ответственности. Будем вносить в КоАП необходимые нормы и надеемся на вашу поддержку.

Различные информационные системы, как действующие, так и перспективные, хранят информацию, необходимую для дальнейшего совершенствования правоохранительной системы Республики Казахстан.

Взаимодействие существующих информационных систем открывает новые горизонты для правоохранительных органов.

Один сотрудник может смотреть видео с 10 камер, но у нас камер десятки тысяч, и для эффективной работы с ними нужны системы видеоаналитики, которые способны самостоятельно выявлять подозрительные ситуации и оповещать об этом операторов.

Обычные планшеты могут превратиться в мощный инструмент, если дать сотруднику полиции возможность эффективно работать с различными системами, уведомлять о срабатывании различных систем оповещения, подключаться к близлежащим камерам.

Например, для выявления опасного водителя на дороге информация должна пройти от камеры, через видеоаналитику и Центр Оперативного Управления, и поступить ближайшему сотруднику полиции по пути следования транспортного средства, и все это должно произойти за секунды

Конечно же, трансформация невозможна без данных. Данные - основа искусственного интеллекта.

На уровне государственных органов ведем большую работу по структурированию данных, описанию. Сейчас выделили домены и по каждому домену совместно с госорганами ведется описание ключевых данных - т.е. например, по воде - нам надо знать сколько водоемов, объемы, характеристики гидротехнических сооружений и т.д.

Это позволит исключить отчеты, запросы разных данных и госорганам станет понятно какие именно данные, кем и с какой периодичностью могут собираться. В идеале, данные должны быть от датчиков и устройств.

Хороший пример, проект «Сергек» – отечественный продукт на основе технологий искусственного интеллекта и машинного обучения. Система собирает необходимые данные по нарушениям. Сейчас развитие продукта идет в сторону сбора данных по запылению и выбросам на улицах городов.

После внедрения АПК «Сергек» смертность при ДТП в г. Астана снизился до 3 человек на 100 тыс. населения и стало наравне с мировыми столицами. В 2022 году смертность при ДТП снизилось до 2 человек на 100 тыс. населения, то есть на 33% меньше, чем в период до начала реализации проекта *(данный показатель рекордно низкий за*

всю историю проекта), а общий уровень правонарушений и преступности в городе Астана в 2022 году снизился на 65%.

Вместе с тем, по данному направлению следует стремиться к достижению нулевого показателя смертности. Это может потребовать обеспечение реализации комплекса мероприятий посредством цифровых инструментов, к примеру, снижение скоростного режима на особо аварийных участках, изменения геометрии улиц, изменение подходов к подготовке водителей общественного транспорта, мероприятия по успокоению трафика и так далее.

В целом работа по реинжинирингу бизнес-процессов государственных органов ведется активно, с переходом от архитектуры государственного органа на единую архитектуру «электронного правительства» на основе доменов *(сфер, отраслей)*.

Пересмотрен процесс государственного контроля и надзора субъектов бизнеса. По итогам реинжиниринга ведется работа по автоматизации системы управления рисков по 35 сферам государственного контроля и надзора, а также разработка **Реестра обязательных требований** по формированию ведения сведений о регуляторных актах.

Так, предусматривается «гибкая» система управления рисками, которая основана на использовании баз данных. Основываясь на данных, данная система будет делить предпринимателей по конкретным степеням риска и формировать списки проверяемых субъектов.

В результате будет обеспечена прозрачность предсказуемость процедур проводимых проверок, снижены издержки бизнеса, недопущение введения необоснованных регуляторных требований для субъектов предпринимательства и так далее.

Выстраивание эффективного процесса по управлению данными ведет к дебюрократизации как для государства, так и для граждан и бизнеса.

Отход от традиционных способов формирования отчетности в сторону обновления данных в режиме реального времени, исключение человеческого фактора, реинжиниринг сбора данных в целях их формирования в цифровом формате позволит вывести государственное управление на принципиально новый уровень.

Будет переход на систему раннего реагирования, когда за счет конкретно определенных рисков неисполнения целевых показателей, посредством аналитики данных можно будет заранее принимать меры до наступления какого-либо происшествия. Это позволит не бороться с последствиями, а устранять причины до их проявления в виде каких-либо негативных происшествий и событий.

С учетом того, что низкое качество данных снижает эффект от цифровизации, важно на системной основе совершенствовать подходы по управлению данными.

Таким образом, политика цифровизации будет формироваться через призму сбора необходимых данных. Синергия политик по управлению данными и цифровой трансформации дадут мультипликативный эффект.

В целях обеспечения Правительства объективными аналитическими данными для принятия эффективных управленческих решений функционирует информационно-аналитическая система «Smart Data Ukimet».

Экосистема «Smart Data Ukimet» позволяет сегментировать и формировать списки потенциальных услугополучателей для оказания государственных услуг проактивно и автоматизировать процессы на основе данных. Наверное вы слышали про проект “цифровая карта семьи”. На базе него уже АСП в плотном режиме переведен на проактивный режим предоставления. Это также снижает риски фальсификации, манипуляций на местах.

Далее предлагаем использовать для всех видов очередей. Это точно позволит исключить человеческий фактор при распределении жилья, автомобилей, очередей в садики.

К примеру, ведутся работы по автоматизации списка присяжных заседателей на базе «Smart Data Ukimet» на основе соответствующих параметров и данных.

В свою очередь, искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека, для целей, определенных человеком, по задачам, которые решаются путем генерации прогнозов, рекомендаций или решений на основе анализа данных и выявленных закономерностей, адаптируемых к среде и влияющих на среду, с которой искусственный интеллект взаимодействует.

На сегодня нет никаких сомнений, что искусственный интеллект – это стратегическая технология, которая быстро растет благодаря увеличению вычислительных мощностей, накоплению большого массива данных и развитию сетей, таких как 5G.

Уже с 2018 года большинством стран разработаны и утверждены стратегии развития искусственного интеллекта.

В настоящее время нами разрабатывается Дорожная карта (стратегическое видение) по развитию искусственного интеллекта.

Изучение международного опыта показывает, что прогнозирование рецидива правонарушений, детекторы аномального поведения, прогнозирование судебного решения входит в число привлекательных сфер для развития искусственного интеллекта.

Необходимо отметить, что в Казахстане в судебную практику элементы искусственного интеллекта внедрены с 2022 года посредством сервиса «Цифровая аналитика судебной практики», разработанного Верховным судом.

Благодаря данному сервису осуществлено упрощение процесса ознакомления с судебной практикой судьями всех уровней.

Сервис позволяет производить поиск судебных актов, по ключевым словам и по смыслу. Программа обучена понимать суть судебных решений, сравнивать их между собой, выявлять аномалии и прогнозировать исход гражданского дела. Имеется возможность при поступлении судье иска видеть судебную практику по схожим делам, вплоть до кассации.

Жалпы, соттарда жасанды интеллектті қолдану айтарлықтай адам ресурстарын босатты, қателіктерді азайтты, сонымен қатар шешім қабылдауға көмектесті.

Цифрлық құралдар құқықтық тәртіпті қамтамасыз етуді, жаңа даму деңгейіне шығаруға мүмкіндік бергенін атап өткім келеді.

Бессонов Алексей Александрович
Ректор Московской академии
Следственного комитета Российской Федерации,
доктор юридических наук, доцент, полковник юстиции,
г. Москва, Российская Федерация

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ: НАСТОЯЩЕЕ И БУДУЩЕЕ

Сегодня технология искусственного интеллекта присутствует буквально на каждом шагу: в наших телефонах, автомобилях, домах. Искусственный интеллект преуспел в медицине, образовании, бизнесе, финансово-кредитной сфере, управлении городами и даже в военных действиях. Высокие вычислительные мощности позволяют машинному интеллекту решать задачи, которые в недавнем прошлом относились к сфере фантастики. Одновременно с этим он приобретает и устрашающие черты. Например, чат-бот ChaosGPT, сообщил о своём желании уничтожить человечество, чему предшествовало исследование им способов уничтожения людей вопреки установленным создателями ограничениям.[1] Известный разработчик искусственного интеллекта из компании Google Джеффри Хинтон в стремительном совершенствовании этой технологии усматривает угрозу для человечества ввиду высокого потенциала её применения в крайне неблагородных целях.[2] Ввиду непредсказуемости систем на основе искусственного интеллекта появляются новые риски, однако наивысшей степени опасности он всё же приобретает в человеческих руках при реализации преступных планов.

Современный криминальный мир использует искусственный интеллект для написания кодов вредоносных программ, взлома пользовательских паролей, хищения денежных средств и персональных данных, генерации фейковых фотографий, аудио- и видеозаписей, посягательства на жизнь и здоровье людей, нарушения суверенитета отдельных государств. Одновременно с этим рассматриваемая технология выступает эффективным инструментом расследования и профилактики криминальных деяний, причём не только киберпреступлений, но и всех других их видов. Достигается это за счёт следующих преимуществ этой технологии:

– высокий потенциал в обработке больших объёмов информации (больших данных, Big Data);

– высокая вычислительная скорость в совокупности с быстродействием современных компьютеров;

[1] Появилась нейросеть, которая хочет уничтожить мир людей // Российская газета. 12.04.2023. № 79 (9024). С. 9.
[2] Человек проиграет // Российская газета. 03.05.2023. № 95 (9040). С. 5.

– возможность работы с цифровыми следами преступлений и в целом с информацией в цифровом формате;

– способность выявления как явных, так и неочевидных закономерностей в данных, представляющих различные явления окружающего мира, сокрытых от невооружённого взгляда человека и иных методов работы с информацией.

В этой связи нами на протяжении уже пяти лет проводится изучение возможностей использования технологии искусственного интеллекта в деятельности по расследованию преступлений. При этом сквозь призму рассматриваемого вопроса как объект исследования искусственный интеллект следует рассматривать, во-первых, как орудие преступлений, а, во-вторых, как инструмент их расследования. Остановимся на втором аспекте.

Пожалуй, наибольшую сложность в расследовании преступлений представляет необходимость принятия решений в условиях постоянной информационной неопределённости, в качестве ключевого средства преодоления которой возможно обозначить моделирование следователем расследуемого преступного деяния и самого процесса расследования. Отметим, что в моделировании искусственный интеллект выступает незаменимым инструментом, позволяя, например, строить поисковый портрет преступника. С целью проверки такой возможности нами предпринято исследование, эмпирическую базу которого составили материалы уголовных дел о более чем 1000 серийных преступлениях, совершённых из сексуальных побуждений 186 преступниками, из числа которых возможно выделить, в первую очередь, Попкова – известного как «ангарский маньяк» (80 преступных эпизодов), Чикатило (58 эпизодов), Макаренкова и Шутова (по 33 криминальных эпизода). Эти деяния совершены в СССР и современной России с 1973 года по 2018 год и включают в себя в том числе 278 серийных убийств, что составляет 26%.

Применение в исследовании методов математической статистики и искусственного интеллекта позволило построить цифровую криминалистическую модель серийных преступлений, содержащую 27 признаков с различным числом градаций, а также выявить закономерные связи между признаками их системы. Закономерности изученных преступлений детерминировали выбор признаков, на основе которых возможно устанавливать серийный характер неочевидных преступлений и причастных к ним лиц. В качестве таких признаков выступили географические координаты места преступления, время совершения деяния (начальное и конечное), вид места преступления, способ и орудия, возраст потерпевшего. Эти признаки преобразованы в доказательственные переменные по методу, предложенному М.Д. Портером[3] и модифицированному нами. Далее модель с

[3] Porter M.D. (2016). A Statistical Approach to Crime Linkage. *The American Statistician*, 70:2, pp. 152–165.

доказательственными переменными протестирована на точность выявления серийных преступлений с помощью таких методов машинного обучения, как наивный байесовский классификатор, логистическая регрессия и градиентный бустинг. В итоге окончательный выбор сделан в пользу алгоритма на основе наивного байесовского классификатора, показавшего точность 92,5–93,1% (*AUC* = 0,969–0,971), и градиентного бустинга (точность 97,7–98,2%, *AUC* = 0,980–0,981)[4]. Причём разработанное программное обеспечение может применяться для работы с различными видами серийных преступлений.

Помимо этого создан алгоритм построения портрета серийного преступника, совершающего свои криминальные деяния по сексуальному мотиву[5], опираясь на ряд признаков, которые устанавливаются следователем, как правило, уже на первоначальном этапе расследования. Эта система базируется на таких алгоритмах искусственного интеллекта, как нейронные сети и градиентный бустинг, и позволяет прогнозировать расстояние от места преступления до места жительства такого преступника, то есть осуществлять географическое профилирование, с точностью 88,3–93,5% (в зависимости от количества используемых интервалов расстояний), его возраст (точность 80,3%, доверительный интервал ±6 лет), наличие у него психического заболевания (точность 81,5%) и судимости (точность 82%), факт совершения преступления с использованием автотранспортного средства и без него (90%), наличие связи между преступником и потерпевшим до совершения деяния (96%), семейный статус – имеется собственная семья или нет (73,8%).

Таким образом, подтверждена гипотеза о возможности использования искусственного интеллекта для: а) построения поискового портрета серийного преступника; б) выявления в массиве нераскрытых деяний тех, которые носят серийный характер и совершены одним и тем же субъектом (выявление связи преступлений); в) установления наиболее вероятного подозреваемого из числа лиц, учтённых в базе данных о преступниках (приоритезация подозреваемого). Исходя из этого, целесообразно продолжать исследования возможностей искусственного интеллекта в моделировании при расследовании различных видов преступлений, в том числе серийного характера.

Следующее направление использования искусственного интеллекта реализуется в поиске и анализе цифровых следов и иной криминалистически значимой информации о расследуемых

[4] Программное обеспечение для выявления серийных преступлений и преступников «crimeserieslinkage» (Свидетельство о государственной регистрации программ для ЭВМ № 2021619836, выдано Федеральной службой по интеллектуальной собственности Российской Федерации 17.06.2021, автор А.А. Бессонов).

[5] Программа для ЭВМ «Портрет серийного преступника “PorSerO”» (Свидетельство о государственной регистрации программ для ЭВМ №2022610749, выдано Федеральной службой по интеллектуальной собственности Российской Федерации 14.01.2022, автор А.А. Бессонов).

преступлениях в виртуальной среде и различных цифровых устройствах. Прежде всего он составляет основу технологии, представленной совокупностью специальных методов и имеющей название «поиск и анализ информации из открытых источников» (OSINT – Open Source Intelligence), в числе преимуществ которой отмечается возможность работы с «большими» и разрозненными (неструктурированными) данными.[6] OSINT заключается в мониторинге с использованием информационно-аналитических методов (Data Mining) открытых источников информационно-телекоммуникационной среды и элементов её инфраструктуры с целью поиска, обнаружения и фиксации криминалистически значимой информации, связанной с подготавливаемым, совершаемым или совершённым преступлением (преступлениями). Поскольку более 60% жителей нашей планеты постоянно оставляют цифровые следы о своей личности и жизнедеятельности, в том числе анкетные данные, фотографии, номера телефонов, сведения о геолокации и т.п., имеющие значение для успешного расследования конкретных преступлений, этот метод является ключевым инструментом установления обстоятельств совершённого деяния и выявления лица, к нему причастного (группы лиц). Высокий потенциал в выявлении информации, имеющей отношение к преступлению и циркулирующей в системах мгновенного обмена сообщениями (мессенджера), прежде всего в Telegram, имеют боты, то есть специальные программы на основе искусственного интеллекта, выполняющие специализированные задачи. Так, используя мессенджер Telegram, можно установить личность интересующего следствие пользователя по его ID и IP-адресу, используемым некнейму, имени и фамилии, номеру телефона, сведениям об устройстве связи, геолокации, фотографиям, связанным с ним другим пользователям, а также по привязанным к нему чатам и каналам, в частности по платёжным реквизитам и отправленным сообщениям.

В качестве примера успешного использования технологии OSINT при работе с Telegram можно привести уголовное дело об убийстве 10 октября 2018 года в посёлке Архангельское Московской области следователя по особо важным делам управления МВД на транспорте по Центральному федеральному округу Шишкиной, несколько месяцев остававшемся нераскрытым. Цифровые следы, оставленные преступниками в Telegram в процессе подготовки этого деяния, позволили установить их личности, включая заказчика.[7]

Технология OSINT применима и к иным сервисам мгновенного обмена сообщениями – WhatsApp, Viber, Signal, ICQ, социальным сетям

[6] Осипенко А.Л. Цифровизация общества и виртуализация реальности: усложнение вызовов и расширение перспектив оперативно-розыскной деятельности // Оперативно-розыскная деятельность в цифровом мире: сборник научных трудов / под ред. В.С. Овчинского. Москва: ИНФРА-М, 2021. С. 164.

[7] Уголовное дело № 2-34/2020, находящееся в архиве Московского областного суда.

и различным сегментам Интернета, в связи с чем требует научной и прикладной проработки для целей оперативно-разыскной и следственной деятельности. В частности, в настоящее время в Московской академии Следственного комитета Российской Федерации проводятся научно-исследовательские работы в этой части.

Ещё одним из важнейших направлений использования искусственного интеллекта в расследовании преступных деяний выступает улучшение качества следов преступления, зафиксированных в цифровом формате. Наиболее ярко это проявляется в работе с видеозаписями камер наружного наблюдения, которые зачастую имеют низкое качество изображения либо фрагментарный характер. К примеру, следствием и судебными экспертами сегодня успешно используются программно-аналитические комплексы, позволяющие идентифицировать человека по изображению фрагмента лица, закрытого маской, установить буквенно-цифровую нотацию государственного регистрационного знака автомобиля, запечатлённого камерой наблюдения под острым углом и потому невооружённым глазом не различимому. Анализ видеоряда записей, осуществлённых разными камерами наблюдения по маршруту движения преступника и прилегающей к месту происшествия территории, предоставляет возможность установить подозреваемого.

Несмотря на это, пока трудноразрешимой и в то же время важнейшей для современного следствия задачей является выявление фэйковых видеоизображения, аудиозаписей и т.п., использованных для их генерации технических и программных средств, изготовивших их лиц. Конечно же исследования в этом направлении идут активно, с акцентированием внимания прежде всего на методах искусственного интеллекта, и их нужно продолжать.

Наконец, необходимо отметить, что методы искусственного интеллекта успешно используются при производстве информационно-аналитических исследований больших объёмов информации, содержащихся в детализациях телефонных соединений, сведениях о финансовых транзакциях, на изображениях видеокамер наблюдения и т.п., позволяя устанавливать связи лиц между собой, их местонахождение, временную линию событий и т.д. Большие перспективы видятся в рассмотрении этой технологии как инструмента при производстве различных судебных экспертиз.

Таким образом, впереди предстоит ещё много поработать на ниве изучения возможностей искусственного интеллекта в расследовании преступлений. Думается, что без объединения усилий специалистов в сфере искусственного интеллекта и расследования преступлений, в том числе на международном уровне, сложно рассчитывать на успех в раскрытии всего возможного потенциала этой технологии в противодействии современной преступности, носящего опережающий

характер по отношению к криминалитету, активно использующему методы машинного обучения в реализации своих преступных замыслов. Большая роль в консолидации возможностей криминалистов и следователей различных стран в таких исследовательских работах должна принадлежать созданному в апреле 2023 года по инициативе Председателя Следственного комитета Российской Федерации Александра Ивановича Бастрыкина Международному союзу криминалистов.

И ещё, на наш взгляд, неизменным спутником всех таких исследований должен быть постулат о том, что искусственный интеллект ни в коем случае не должен рассматриваться применительно к сфере уголовного судопроизводства как замена человека, но исключительно как инструмент повышения его возможностей, способностей и человеческого потенциала.

Ахметзакиров Наиль Рафисович,
Руководитель Судебной администрации Республики Казахстан,
г. Астана, Республика Казахстан

ЭЛЕМЕНТЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И РОБОТИЗАЦИЯ В СУДОПРОИЗВОДСТВЕ: ТРЕНДЫ И ПЕРСПЕКТИВЫ

Независимость судебной власти, доверие к судам, справедливость, открытость и прозрачность правосудия – постулаты всем известные и они не раз обсуждались.

Но предлагаю взглянуть на них под другим углом.

Может ли классическое правосудие существовать в отрыве от больших инновационных сдвигов?

Сейчас, когда свою жизнь и здоровье мы зачастую доверяем компьютеру, а финансами в банке управляют бездушные роботы, как Вы думаете:

– Насколько глубоко цифровизация может проникать в процесс отправления правосудия?

– Робот-судья: это, по-прежнему, фантазии или неизбежная перспектива будущего?

Эти вопросы сами ворвались в нашу жизнь. Мы не раз их обсуждали на встречах различного уровня.

Жить онлайн для всех нас стало нормой.

Все привыкли получать информацию в один клик.

Качественно и быстро стало не ожиданием, а требованием времени.

Поэтому, изучая опыт наших зарубежных коллег, можно сделать вывод, что цифровизация безальтернативно ворвалась и в нашу работу.

Доступность интернета и масштабная оцифровка государственных баз данных позволили перевести судопроизводство на электронные рельсы.

Весь кейс по всем видам судопроизводства формируется электронно. Самым сложным стало внедрение электронного уголовного дела. В 2018 году начали с одноэпизодных дел небольшой тяжести. В течение первых трёх лет доля е-уголовных дел выросла с 15 до 30%.

Со второго полугодия прошлого года органы следствия практически полностью перешли на электронный формат ведения уголовных дел. Их удельный вес по итогам года составил уже 73%.

В 2023-2024 годах ожидаем 100-процентное поступление уголовных дел в электронном виде.

В цифрах в нашей системе ежеминутно формируется более 100 новых документов.

Второе.

Этим гигантским постоянно растущим информационным массивом нужно было научиться управлять.

Для этого создали Ситуационный центр.

Соответствующие программы и алгоритмы позволяют видеть каждый материал в суде с момента его поступления и в режиме реального времени и автоматически формировать десятки аналитических справок: о соблюдении процессуальных сроков, судебной нагрузке, категориях дел и многое другое.

Данные по 850 показателям доступны как в целом по республике, так в разрезе регионов и конкретных даже самых отдалённых судов.

Иными словами, мы можем получить любую интересующую нас информацию с аналитическими выкладками по заданным параметрам.

Третье. Доступ к судам.

Открыли единое электронное окно доступа.

Через **«электронный Судебный кабинет»**, который есть и в мобильной версии, пользователи из любой точки мира, где есть интернет, могут обратиться в наши суды.

Если в 2015 году в электронном виде подавалось всего 5% исков, то сегодня этот показатель достиг 90%.

При этом оставшиеся 10%, поступающих нарочно, сканируются и дальше рассматриваются по алгоритмам электронного судопроизводства.

Процессы также могут проходить в онлайн-формате.

Ежегодно фиксируем подачу исков и участие представителей более чем из 30 государств мира.

Понимание того, что суд больше не привязан к конкретной географической территории, позволило ввести в гражданское судопроизводство **экстерриториальную подсудность.**

Её запуск состоялся 1 августа 2022 года.

Теперь участники процесса вправе судиться не в месте своего географического проживания, а в любом другом суде нашей страны.

В какой суд попадёт спор, определяет роботизированная программа, которая не делит суды на районы и области.

По нашему мнению дальнейшее развитие экстерриториальной подсудности имеет очевидные плюсы.

Первое. Уровняется нагрузка судей, которая в крупных городах превышает объем сельских районов в десятки раз.

Второе. Снизятся коррупционные риски. Учитывая автоматизированное распределение дел в другие регионы нашей республики, суждения о возможном влиянии местных органов власти и бизнес-элиты на суд должны уйти в прошлое.

Третье. Более эффективно будут использованы трудовые и материальные ресурсы.

Можно ли это назвать Суд будущего?

Пока ответить на это сложно, ведь даже навскидку возникает масса вопросов.

Хотя бы о соответствии такого решения международным требованиям о непосредственности участия в суде и др.

Но скорость цифрового прогресса подсказывает, что тема сама по себе актуальна.

В подтверждении этому разрешите презентовать две наши последние разработки.

Первая – это **Цифровая судебная аналитика**, разработанная по поручению Главы государства.

Именно она должна стать помощником в формировании единообразной судебной практики.

Отличительной особенностью этого IT-продукта является применение элементов искусственного интеллекта.

Сервис позволяет, как в Google, найти любую информацию в тексте всех состоявшихся с 2018 года судебных актах. Копилка пополняется ежедневно.

Аналитические фильтры одним кликом позволяют выбрать регион, суд, судью, категорию дела и т.д. для быстрого поиска интересующих судебных решений.

Система демонстрирует, какое количество найденных по конкретному запросу решений обжаловались в апелляции и сколько стали предметом рассмотрения в Верховном Суде.

Доступ к нужной информации и её анализ позволят каждому судье сориентироваться в судебной практике по любому находящемуся в производстве делу.

Помимо простого есть интеллектуальный поиск.

Почему интеллектуальный?

Поисковик ищет не по словам, а по ситуации.

То есть программа обучена понимать суть судебных решений, сравнивать их между собой, выявлять аномалии и прогнозировать исход по гражданским делам.

Допустим, судью интересует практика по конкретному иску, который содержит массу аргументов и нюансов. Если ввести текст иска в поисковик, система автоматически найдет все максимально схожие дела, с результатами их обжалования.

Более того, Программа показывает решения, явно выбивающиеся из судебной практики.

Основным достижением работы искусственного интеллекта является возможность прогнозирования исходов гражданского дела. Сейчас данный сервис активно используется судьями. В перспективе рассчитываем, что аналогичные программы станут доступными для населения и адвокатов.

Второй IT-продукт, используемый с прошлого года - это роботизация не сложных процессов.

На основе четких алгоритмов принятия решений робот готовит проекты судебных актов по делам, где судейское усмотрение строго ограничено законом.

К примеру, дача санкции, запрещающая должнику покидать страну.

Несмотря на трудозатратность проверок всех документов, ни какой правовой сложности в принятии решения нет.

Судья не оценивает доказательства, не применяет судебную практику и не исследует нормы права.

По нашим законам в течение 3^x дней он должен проверить наличие долга, превышающего примерно 250 евро и надлежащее заблаговременное уведомление должника. Если оба эти условия соблюдены – санкция дана, если нет – отказ.

Мы интегрировали соответствующие базы данных, и сейчас робот готовит проект такой санкции через минуту после поступления материала. При этом ответственность при подписании решения сохраняется за судьей. Конституционные требования не нарушаются.

Сейчас анализируем категории дел и материалов, имеющих потенциал для дальнейшей роботизации.

Таким образом, с одной стороны суды разгружаются от рутины, а с другой - минимизируются судебные ошибки.

Для законодательного урегулирования этого вопроса внесены поправки в ГПК, предусматривающие возможность создания проектов судебных актов информационной системой.

При этом важно понимать, что внедряемые нами технологии не заменят судью-человека.

Это лишь дополнительный инструмент помощи для обеспечения единообразия судебной практики и качественной защиты прав участников процесса.


ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ
ЖАСАНДЫ ИНТЕЛЛЕКТ: ҚҰҚЫҚТЫҚ РЕТТЕУ МӘСЕЛЕЛЕРІ
ARTIFICIAL INTELLIGENCE: PROBLEMS OF LEGAL REGULATION

УДК 004.8:34

Беляева Лариса Ивановна
Профессор кафедры уголовной политики Академии управления
МВД России, заслуженный юрист Российской Федерации,
доктор юридических наук, профессор,
г. Москва, Российская Федерация

МЕСТО И РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООТНОШЕНИИ

Аннотация. Тема искусственного интеллекта в настоящее время является одной из самых обсуждаемых, что вполне объяснимо: новые технологии вошли в нашу жизнь, они развиваются, меняют её. Они, порой, меняют устоявшиеся правила и стереотипы поведения. Использование технологий искусственного интеллекта – требование времени.

Появление и использование систем искусственного интеллекта по –разному воспринимается и оценивается гражданами и профессиональными сообществами, в том числе правовым. У одних открывающиеся возможности вызывают восторг, у других – настороженность и опасения в связи с возможными, а порой неизбежными, нарушениями прав граждан и организаций, в частности в области обеспечения их информационной безопасности.

Однако жизнь не остановить. Технологии искусственного интеллекта, как говорят, уже в пути. Они находят место и в правоприменительной деятельности. Эта практика расширяется. Использование технологий искусственного интеллекта в правоприменительной практике является неизбежным.

Но вопрос состоит в том, что четкого правового регулирования применения этих технологий пока нет. В связи с этим насущной задачей является определение пределов и возможностей использования технологий искусственного интеллекта в правоприменительной практике, в том числе судейской.

Много вопросов возникает в связи с правовой оценкой результатов самостоятельной деятельности технических аппаратов, носителей искусственного интеллекта.

Поскольку правоприменение – это система правоотношений, представляется целесообразным подойти к вопросу правового регулирования с позиций учения о правоотношении, что может способствовать пониманию проблем правового регулирования в указанной сфере и путей их решения.

Ключевые слова: искусственный интеллект; правосубъектность; правоотношение; субъект права; права и обязанности; субъект правоотношения; правовое регулирование.

Аннотация. Жасанды интеллект тақырыбы қазіргі уақытта ең көп талқыланатын тақырыптардың бірі болып табылады, бұл түсінікті: біздің өмірімізге жаңа технологиялар енді, олар дамып, оны өзгертуде. Олар кейде қалыптасқан ережелер мен мінез-құлық стереотиптерін өзгертеді. Жасанды интеллект технологияларын қолдану – уақыт талабы.

Жасанды интеллект жүйелерінің пайда болуы мен қолданылуын азаматтар мен кәсіби қауымдастықтар, соның ішінде заңгерлік қауымдастықтар әртүрлі қабылдайды және бағалайды. Кейбіреулер үшін ашылған мүмкіндіктер қуаныш тудырады, басқалары үшін - азаматтар мен ұйымдардың құқықтарын, атап айтқанда

олардың ақпараттық қауіпсіздігін қамтамасыз ету саласындағы ықтимал, кейде болмай қоймайтын бұзушылықтарға байланысты сергектік пен қорқыныш.

Дегенмен, өмірді тоқтату мүмкін емес. Жасанды интеллект технологиялары келе жатыр деп айтылады. Олар да құқық қорғау органдарында өз орындарын табады. Бұл тәжірибе кеңейіп келеді. Құқық қолдану тәжірибесінде жасанды интеллект технологияларын пайдалану сөзсіз.

Бірақ мәселе бұл технологияларды қолданудың нақты құқықтық реттеуі әлі жоқ. Осыған байланысты құқық қолдану тәжірибесінде, оның ішінде сот тәжірибесінде жасанды интеллект технологияларын қолданудың шектері мен мүмкіндіктерін анықтау кезек күттірмейтін міндет болып табылады.

Техникалық құрылғылардың, жасанды интеллект тасымалдаушылардың дербес қызметінің нәтижелерін құқықтық бағалауға байланысты көптеген сұрақтар туындайды.

Құқық қорғау қызметі құқықтық қатынастар жүйесі болғандықтан, құқықтық реттеу мәселесіне осы саладағы құқықтық реттеу мәселелерін және оларды шешу жолдарын түсінуге ықпал ете алатын құқықтық қатынастар доктринасы тұрғысынан қараған дұрыс сияқты.

Түйінді сөздер: жасанды интеллект; заңды тұлға; құқықтық қатынас; құқық субъектісі; құқықтары мен міндеттері; құқықтық қатынас субъектісі; құқықтық реттеу.

Annotation. The topic of artificial intelligence is currently one of the most discussed, which is understandable: new technologies have entered our lives, they are developing, changing it. They, at times, change the established rules and stereotypes of behavior. The use of artificial intelligence technologies is a requirement of the time.

The emergence and use of artificial intelligence systems is perceived and evaluated differently by citizens and professional communities, including legal ones. For some, the opening opportunities cause delight, for others - alertness and fears in connection with possible, and sometimes inevitable, violations of the rights of citizens and organizations, in particular in the field of ensuring their information security.

However, life cannot be stopped. Artificial intelligence technologies are said to be on the way. They also find a place in law enforcement. This practice is expanding. The use of artificial intelligence technologies in law enforcement practice is inevitable.

But the question is that there is no clear legal regulation of the use of these technologies yet. In this regard, an urgent task is to determine the limits and possibilities of using artificial intelligence technologies in law enforcement practice, including judicial practice.

Many questions arise in connection with the legal assessment of the results of the independent activity of technical devices, carriers of artificial intelligence.

Since law enforcement is a system of legal relations, it seems appropriate to approach the issue of legal regulation from the standpoint of the theory of legal relations, which can contribute to understanding the problems of legal regulation in this area and ways to solve them.

Keywords: artificial intelligence; legal personality; legal relationship; subject of law; rights and obligations; subject of legal relationship; legal regulation.

Развитие и активное внедрение в жизнь современных технологий обусловливает трансформацию многих сторон социальной жизни. Не осталась в стороне и правовая жизнь общества, в которой известную роль играют информационные системы, в том числе искусственный интеллект. Как отмечают исследователи, в настоящее время термин «искусственный интеллект» не имеет устойчивого единства и им

обозначаются разнообразные технологии, преимущественно те, которые связаны с искусственными нейронными сетями [1,5 -15].

Представляется, что появление словосочетания «искусственный интеллект» является следствием пренебрежения к языковым нормам и правилам. Это получило довольно широкое распространение в настоящее время. Результатом этого является конструирование таких терминов, которые с точки зрения языковых норм неверны. Так, следуя моде на «цифру», стали говорить о цифровом правосудии, цифровой преступности, цифровом полицейском, киберправосудии. И подобных терминов в настоящее время существует великое множество. При этом каждый из авторов понимает под этими терминами нечто свое, хотя каждое слово имеет свою смысловую нагрузку. Это же произошло с интеллектом. Это говорит о необходимости более тесного сотрудничества инженеров с филологами и юристами.

Интеллект - свойство живого организма, данное ему от природы – человека. То есть, говоря об искусственном интеллекте, свойство человека переносится на некое техническое средство, механизм, аппарат.

Интеллект человека позволяет ему осуществлять мыслительную деятельность, принимать решения, нести за них ответственность. Нельзя сказать, что это же является свойством механизма, аппарата, робота, искусственного интеллекта. Как совершенно правильно отмечает Ю.А. Цветков, искусственный интеллект-это имитация того, что программисты представляют себе как человеческий интеллект. То есть они реализуют свои представления об интеллекте, а не создают его. Это сделать и невозможно [2, 91-107].

Как следует из Указа Президента РФ от 10 октября 2019 г. №490 «О развитии искусственного интеллекта в Российской Федерации», искусственный интеллект представляет собой комплекс технологических решений, позволяющих имитировать когнитивные функции человека, в том числе самообучение и поиск решений без заранее заданного алгоритма, и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека [3]. Т.е. в названном документе прямо говорится о том, что искусственный интеллект на самом деле вовсе не интеллект в общепринятом смысле, а лишь его имитация, подделка.

Очевидно, что искусственный интеллект открывает новые неисчерпаемые возможности в социальной жизни.

Вместе с тем его использование не столь безобидно, как может показаться. Более того, он рассматривается как источник повышенной опасности [4, 638-708]. Это объясняется очень просто: его возможности пока не определены, на определенном этапе применения он становится неуправляемым и не поддается контролю.

Специалисты отмечают, что серьезные опасения вызывает технология создания цифровых копий людей, как живых, так и умерших. Созданный двойник посредством искусственного интеллекта может стать виртуальной копией конкретного человека, которая может генерироваться в различных форматах. Пересечение многих слоев сведений, которые накапливаются в аппарате носителе искусственного интеллекта, позволяют создавать вполне реалистичные по форме и способу выражения, но фейковые по сути, сведения и изображения. Это открывает неограниченные возможности различных монтажей и распространения недостоверной или искаженной информации и создания таким образом разного рода конфликтных ситуаций.

Заслуживает внимания система хранения персональных данных. Изначально её создание преследует благородные цели ускорения предоставления услуг, упрощения решения актуальных вопросов. Нет нужды говорить о тех проблемах и опасностях, которые возникают с утечкой информации [5,79-84]. Все это приводит к выводу о том, что условия, пределы и порядок использования искусственного интеллекта в правоприменительной практике должны быть четко определены нормами права.

Поскольку правоприменительная деятельность представляет собой систему, совокупность правоотношений, есть смысл проанализировать положение технологии искусственного интеллекта в правоотношении. И здесь мы обнаруживаем, что таких правоотношений не очень много. Поскольку использование технологий искусственного интеллекта нормами права не урегулировано. Именно поэтому так активно обсуждается вопрос о роли системы искусственного интеллекта в правоотношениях [6,12-31; ,63-72; 8,20-26].

Как известно, для правоотношения характерным является наличие у сторон субъективных юридических прав и обязанностей, которые устанавливаются соответствующими правовыми нормами. Правоотношение – всегда двусторонняя связь. Содержание правоотношения составляют субъективные юридические права и обязанности. Субъективное юридическое право складывается из трех правомочий: на собственные действия, на требование от другой стороны исполнения обязанности, на притязание.

Известно, что нейросетевое программное обеспечение аппарата-носителя искусственного интеллекта является результатом творческой деятельности физического лица или группы лиц) – программиста (программистов). Именно они и являются носителями субъективных юридических прав и обязанностей.

Однако на определенном этапе развитие этого программного обеспечения возможно и без участия и влияния автора (авторов). То есть сам аппарат может производить новую информацию, причем непредсказуемо. При этом техническое средство, аппарат, механизм, в

котором заключен искусственный интеллект, не является носителем субъективных юридических прав и обязанностей, поскольку не обладает для этого необходимыми качествами.

В связи с этим возникают вопросы, связанные с объектом правоотношения. С одной стороны - это программа, позволившая аппарату функционировать, а с другой - новая информация, созданная самим аппаратом.

В первом случае носителем субъективных прав является программист, составивший программу. А вот к новой информации, созданной аппаратом, он имеет опосредованное отношение. Таким образом, возникает следующие проблемы:

а) оценка новой, созданной аппаратом информации, как юридического факта, способного вызвать, изменить или прекратить правоотношение. Такая оценка невозможна, если это не предусмотрено правовыми нормами. Из этого положения следует, что такая информация может создаваться и существовать без всяких пределов и правил, что создает угрозу охраняемым законам интересам участников правоотношений;

б) определение наличия субъекта правоотношения, в частности, установления:

- реальности и достоверности интеллектуального компонента;
- наличия волевого компонента, позволяющий создавать новую информацию.

Субъект правоотношения должен обладать правосубъектностью: правоспособностью, дееспособностью и деликтоспособностью. Таким качеством обладает лицо (физическое или юридическое). В нашем случае это программист (программисты). Однако их правосубъектность не распространяется на ту информацию, которая создавалась техникой без их участия.

В связи с этим возникает вопрос о роли искусственного интеллекта в правоотношении. И его решение не просто и не однозначно [9,94-109]. Очевидно, что новая информация, произведенная уже без участия человека и его интеллекта, волевых усилий и самоконтроля, может носить различный характер и оказывать не контролируемое влияние на людей.

Системы искусственного интеллекта (роботы) не могут, не способны воспринимать и реализовывать этические и правовые нормы. То есть, они не смогут соблюсти этические и нравственные ориентиры, предписания правовых норм, касающиеся охраны прав участников правоотношений на неприкосновенность частной жизни, угрозы и вызовы которым возникают в процессе реализации новой информации, созданной без участия человека[10,238-248].

Из этого вытекает вопрос, связанный с последствиями воздействия на общественные отношения той информации, которая была

произведена самим аппаратом и которая причинила вред этим отношениям. То есть это вопрос о юридических обязанностях, возникающих в связи с распространением информации, произведенной аппаратом носителем искусственного интеллекта. Как показывают исследования, этот вопрос является довольно сложным, не имеющим простых решений и требующим глубокой правовой проработки [4, 638-708].

Искусственный интеллект уже активно используется в различных областях правоприменения, в том числе в правосудии [11,12-16; 12,61-85; 13,15-20; 14,160-168; 15,37-42; 16,17-20]. Специалисты по разному оценивают практику и возможности использования технологий искусственного интеллекта в судейском деле, по преимуществу, это рассматривается как возможность разгрузить судей от текущих дел или как возможность заменить судью как такового. Вместе с тем высказываются и предостережения от опасностей в этой области [17,17-21].

Очевидно, что многие проблемы и вопросы, связанные с использованием технологий искусственного интеллекта, проистекают из неполноты правового регулирования этого процесса.

Право, как известно, регулирует общественные отношения, отношения между людьми. Его социальная роль состоит в том, чтобы защитить участников правоотношений от посягательств на их субъективные права. Именно для этого устанавливается юридическая обязанность в виде ответственности за допущенные нарушения. Все это возможно, если правоотношение возникло, существует, определены юридические факты, лежащие в его основе; его субъекты установлены. Однако правоотношение при отсутствии нормы права невозможно. Поэтому в целях упорядочения процесса применения технологий искусственного интеллекта, важно его правовое обеспечение. Необходимо выработать единые подходы к использованию технологий искусственного интеллекта, систематизировать направления и формы его внедрения в правоприменительную практику, в том числе правосудие [18,47-58]. Безусловно, четко должно быть определено положение искусственного интеллекта в правоотношении, возникающем в правоприменительной практике. Представляется, что его назначение состоит в обеспечении, упорядочении управленческих функций, организационном обеспечении деятельности правоприменителя. При этом субъектом правоотношения может быть только правоприменитель – человек. Механизм, содержащий в себе искусственный интеллект, всего лишь помощник, техническое средство, позволяющее оптимизировать, ускорить, усовершенствовать работу. Именно поэтому необходимы пределы его использования. Юридическая ответственность за характер деятельности механизма – удел правоприменителя. Его обязанность состоит в том, чтобы не прибегать к недозволенному,

контролировать процесс в интересах обеспечения защиты прав участников правоотношения.

Список использованных источников:

1. Черногор Н.Н. Искусственный интеллект и его роль в трансформации современного правопорядка. // Журнал российского права. 2022. №4. С.5-15.
2. Цветков Ю.А. Искусственный интеллект в правосудии. // Закон. 2021. №4. С. 91-107.
3. Указ Президента РФ от 10 октября 2019 г. №490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030года»)// СЗ РФ.2019. №41. Ст.5700.
4. Харитонова Ю.С., Савина В.С., Паньини Ф. Гражданско-правовая ответственность при разработке и применении систем искусственного интеллекта и робототехники: основные подходы. // Вестник Пермского университета. Юридические науки. 2022. №4. С. 683-708.
5. Альбицкая И., Косяков А. Искусственный интеллект для юристов. // Юридический справочник руководителя. 2022. №1. С.79-84.
6. Афанасьев С.Ф. К проблеме материальной и процессуальной правосубъектности искусственного интеллекта. // Вестник гражданского процесса. 2022. №3. С.12-31.
7. Шахназаров Б.А. Правовое регулирование отношений с использованием искусственного интеллекта. // Актуальные проблемы российского права. 2022. №9. С. 63-72.
8. Таран К.К. Предпосылки правового регулирования результатов интеллектуальной деятельности, созданных с использованием искусственного интеллекта. // Право и экономика.2023.№1.С.20-26.
9. Чаннов С.Е. Робот (система искусственного интеллекта) как субъект (квазисубъект) права. // Актуальные проблемы российского права. 2022. №12. С. 94-109.
10. Камалова Г.Г. Этические и правовые вопросы охраны права на неприкосновенность частной жизни при создании и использовании робототехники и систем искусственного интеллекта // Информационное пространство: обеспечение информационной безопасности и право: Сб. науч. трудов / Под ред. Т.А. Поляковой, В.Б. Наумова, А.В. Минбалеева. М.: ИГП РАН. 2018. С. 238-248.
11. Козырева А.А., Пирожкова Т.В. Применение технологий искусственного интеллекта в правосудии // Администратор суда. 2021. №2. С. 12-16.
12. Мохат П.М. Применение искусственного интеллекта в судебном процессе.// Вестник гражданского процесса.2019.№3.Т.9.С.61-85.
13. Сычева О.А. Здравый смысл в судебном доказывании.//Российский судья.2019№8.С.15-20.
14. Заплатина Т.С. Искусственный интеллект в вопросе вынесения судебных решений, или ИИ-судья. // Т.С. Заплатина // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. №4(56). С. 160-168.
15. Курочкин С.А. О перспективах применения искусственного интеллекта в гражданском и арбитражном судопроизводстве.// Арбитражный и гражданский процесс.2023.№2.С.37-42.
16. Дробышева А.В. Перспективы использования технологий искусственного интеллекта в системе мировых судов. // Мировой судья. 2022. №11. С.17-20.
17. Малина М.А. Мировая юстиция и искусственный интеллект.// Мировой судья.2021.№4.С.17-21.

18. Макутчев А.В. Современные возможности и пределы внедрения искусственного интеллекта в систему правосудия. // Актуальные проблемы российского права. 2022. №8. с.47-58.

УДК 004.8:34

Горошко Игорь Владимирович
заведующий отделом правовой статистики и информационного обеспечения прокурорской деятельности Университета прокуратуры Российской Федерации, доктор технических наук, профессор, старший советник юстиции
г. Москва, Российская Федерация

ЭТИКА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В статье поднимаются актуальные вопросы внедрения этических принципов в системы искусственного интеллекта. Анализируются различные направления применения искусственного интеллекта в сфере правоохраны и связанные с этим проблемы. Рассматриваются угрозы использования технологии искусственного интеллекта в противоправной деятельности. В заключительной части автором делается вывод о необходимости отказа в системах «сильного» искусственного интеллекта от преимущественной ориентации на принципы аналитической этики и осуществления перехода к этике феноменологической.
Ключевые слова: информационные технологии; искусственный интеллект; правоохранительная деятельность; этика.

Аннотация. Мақалада жасанды интеллект жүйелеріне этикалық принциптерді енгізудің өзекті мәселелері көтеріледі. Құқық қорғау саласында жасанды интеллектті қолданудың әртүрлі бағыттары және соған байланысты проблемалар талданады. Жасанды интеллект технологиясын заңсыз әрекетте қолдану қаупі қарастырылуда. Қорытынды бөлімде автор «күшті» жасанды интеллект жүйелерінде аналитикалық этика принциптеріне басымдық беруден және феноменологиялық этикаға көшуді жүзеге асырудан бас тарту қажеттілігі туралы қорытынды жасайды.
Түйінді сөздер: ақпараттық технологиялар; жасанды интеллект; құқық қорғау қызметі; этика.

Annotation. The article raises current issues of implementing ethical principles in artificial intelligence systems. Different directions of application of artificial intelligence in the sphere of law enforcement and related problems are analyzed. The threats of using artificial intelligence technology in illegal activities are considered. In the final part the author concludes that it is necessary to abandon the predominant orientation on the principles of analytical ethics in the systems of "strong" artificial intelligence and implement a transition to phenomenological ethics.
Keywords: information technology; artificial intelligence; law enforcement; ethics.

Вопросам, связанным с этикой использования информационных технологий вообще и ИИ (далее – ИИ), в частности, сегодня уделяется большое внимание во многих странах мира.

Первые кодексы, содержащие этические нормы взаимоотношений: программист-компьютер-пользователь, были разработаны в Соединенных штатах Америки (далее – США) ещё в конце прошлого

века. Они носили достаточно декларативный характер и отражали точку зрения отдельных специалистов, решавших, что есть хорошо, а что плохо в новой информационной реальности, но с учетом традиционных ценностей.

В частности, нормы «Не используй компьютер для воровства» или «Не присваивай чужую интеллектуальную собственность» созвучны восьмой христианской заповеди «Не укради» [1].

Бурное развитие информационно-коммуникационных технологий и их внедрение в различные сферы человеческой деятельности сопровождалось появлением специализированных кодексов, адаптированных под эти сферы.

Например, в России, в электронной коммерции используется «Этический Кодекс участника IT-рынка» [2], в сфере телемедицины – «Кодекс этики врачей Рунета» [3] и т.п.

Анализ вышеназванных и некоторых других кодексов позволяет сделать вывод о стремлении их авторов убедить окружающих в несовершенстве новой информационной этики и, словно возрождая идеи Декарта и Гоббса, проповедовать её рациональность, призвать сосредоточить усилия на выработке четких моральных критериев, разграничивающих добро и зло, справедливость и несправедливость.

С появлением технологии искусственного интеллекта сложившиеся подходы к пониманию новой этики требуют своего переосмысления.

Почему это так необходимо? Дело в том, что, как предсказывают, в недалеком будущем системы ИИ будут способны не только помогать человеку принимать решения, но и генерировать решения самостоятельно, в том числе и касающиеся самого человека.

Поэтому, осознав недостаточную изученность и сложность проблемы, исследователи перешли от превалирующей аналитичности в подходах к формулированию ценностных установок и принципов, которым необходимо следовать на всех этапах жизненного цикла искусственных интеллектуальных систем.

Цель этих установок и принципов – создать основу для позитивного развития систем ИИ в интересах личности, общества, государства и окружающей среды.

Как подчеркивается в Рекомендациях об этических аспектах искусственного интеллекта, подготовленных Генеральной конференцией ЮНЕСКО в 2021 году, названные ценности и принципы призваны содействовать защите и уважению прав и основных свобод человека, равенства, включая равенство мужчин и женщин, обеспечению соблюдения интересов нынешнего и будущих поколений, сохранению окружающей среды, биоразнообразия и экосистем, а также уважению культурного разнообразия [4].

В Кодексе этики в сфере искусственного интеллекта, разработанном в Российской Федерации в 2021 году, в число принципов

также вошли: уважение автономии и свободы воли человека в сочетании с требованием к разработчикам следовать закону на всех этапах создания, внедрения и использования систем ИИ [5].

Представляется, что названные принципы приобретают особое значение в правоохранительной деятельности, поскольку она при конкретных обстоятельствах самым непосредственным образом затрагивает права и свободы человека и гражданина, общественную и государственную безопасность.

В этой сфере можно выделить несколько проблемных аспектов, каждый из которых оригинально проявляет себя в определенных направлениях использования ИИ.

Прежде всего нельзя не остановиться на системах ИИ, основное предназначение которых состоит в построении логических выводов или правил, формируемых в результате последовательного осуществление этапов сбора, передачи, хранения и обработки так называемых больших данных (далее - Big Data).

В общем случае под Big Data понимаются большие объемы информации (до сотен петабайт, в том числе и неструктурированной), генерируемые с большой скоростью.

На каждом этапе работы с такими данными существует серьезная опасность допустить критическую ошибку, способную подорвать доверие к искусственному интеллекту.

Так, на этапах сбора, передачи и хранения данных возможна их утечка, что приведет к дискредитации института защиты персональных данных.

Такие данные могут стать доступны злоумышленникам, которые способны использовать их в целях манипулирования, шантажа, мошенничества и т.п.

Ошибка возможна и на этапе аналитической обработки данных, как следствие некорректной работы используемых алгоритмов, в том числе написанных на популярном сегодня Phyton.

Например, справедливой критике подвергаются различные системы, с помощью которых оценивается вероятность рецидива преступления, построенные на основе анализа анкет, которые заполняют заключенные.

Помимо того, что применяемые в них алгоритмы достаточно сложны и непрозрачны, специалисты отмечают некорректность вопросов анкеты, ответы на которых во многом зависят от уровня образования, социального статуса и возраста опрашиваемых, т.е. априори предполагают неравенство последних [6].

Некоторая предвзятость присутствует и в системах, ориентированных на прогнозирование преступности на определенной территории. Такие прогнозы строятся по результатам анализа больших данных, аккумулирующих факты преступного поведения за предыдущие

периоды, локации этих фактов, тяжесть совершенных преступных деяний и т.п. Как показывает практика, подобным образом сконструированные прогнозные системы в основном сосредотачиваются на отслеживании ситуации в бедных районах городов, в то время как богатые кварталы выпадают из-под их контроля.

Отмеченные ошибки поддаются исправлению – в действующие алгоритмы вносятся соответствующие корректировки.

Гораздо большую проблему представляет собой всё нарастающее осознанное непонимание необходимости такого объема данных и гносеологические проблемы, связанные с их использованием. В этом случае подтверждается справедливость давно известного в физике постулата: «естественная эволюция любой системы соответствует убыли информации, т.е. росту энтропии» [7]. С тем, что развитие систем ИИ по своему характеру очень напоминает эволюционный процесс, вряд ли кто будет сегодня спорить.

Говоря об этических проблемах систем ИИ в правоохранительной деятельности, следует остановиться на тех из них, которые связаны с распознаванием фотографий, а также видео- и аудиорядов.

Возможные при этом ошибки бывают заложены, как и для ранее рассмотренных систем, уже в самих алгоритмах распознавания, поскольку используемые в них метрики похожести предполагают наличие пороговых значений.

Однако, нередки случаи, когда необоснованность выводов систем ИИ провоцируется нетолерантной позицией разработчиков, их предубеждением по отношению к различным формам проявления человеческого бытия.

Поэтому неслучайно, что в уже упоминаемых Рекомендациях об этических аспектах искусственного интеллекта специально подчеркивается, что субъекты, связанные с ИИ деятельности должны прилагать максимум усилий, чтобы минимизировать проявления в жизненном цикле системы ИИ дискриминационных способов их применения (дискриминационных по расовой принадлежности, гендерной принадлежности, национальности, социальному происхождению, вероисповеданию, политическим или иным убеждениям, цвету кожи, возрасту, языку, условиям рождения, физическим недостаткам и любым иным факторам).

Актуальной проблемой для правоохранительной деятельности в последние годы становится применение систем ИИ, работающих с голосовыми рядами и видеоизображениями, в противоправных целях.

Здесь речь, прежде всего, идет о технологии так называемых дипфейков (от англ. Deepfake – *хорошо (глубоко) скрытая неправда, ложь*).

Данная технология позволяет заменить фотографию, голос и видеоизображение конкретного человека искусно выполненной

подделкой, синтезированной с помощью нейронных сетей. Изобретенная в 2014 году в виде особого алгоритма, на первом этапе, она использовалась в масштабных розыгрышах и в индустрии развлечений. В дальнейшем область её применения распространилась на производство рекламы (в том числе. политической) и видеоконтента «для взрослых». В первом случае известные люди, такие, например, как Марк Цукерберг, Илон Маск или Барак Обама, с экрана телевизора произносили не принадлежащие им речи (при этом компьютер воспроизводил не только голос, но даже оригинальную артикуляцию). Во втором случае лицо одного человека встраивалось в соответствующую видеозапись, изображавшего поведение другого.

Первые дипфейки производились отдельными энтузиастами, отличались невысоким качеством, и установить подделку можно было, не прибегая к сложным исследованиям.

Сегодня данная технология переживает бурное развитие, на рынке появилось большое число сервисов (например, FakeApp, Zao, Neural Rendering, GPT и др.), которые сделали дипфейки доступными обычным пользователям. При этом качество современных дипфейков существенно выросло.

Противоправными целями использования дипфейков являются:

– хулиганство;

– мошенничество;

– политические, социальные и экономические провокации, приводящие
к дестабилизации социально-экономической обстановки как внутри страны, так и за рубежом и т.п.

Потенциально угрозы, связанные с дипфейками, представляют опасность и могут нанести ущерб:

– чести и достоинству личности;

– конституционным правам и свободам человека и гражданина;

– общественной безопасности и общественному порядку;

– общественной нравственности;

– международным отношениям и т.п.

В этих условиях перед правоохранительными органами стоит непростая задача научиться противостоять таким угрозам. Первые шаги в этом направлении уже сделаны. Так, в 2021 году Министерством внутренних дел Российской Федерации (далее - МВД России) в лице Федерального казенного учреждения «Научно-производственное объединение «Специальная техника и связь» объявило конкурс на выполнение научно-исследовательской работы «Исследование возможных способов выявления признаков внутрикадрового монтажа изображений, выполненного с помощью нейронных сетей». Соответствующее объявление было размещено на официальном сайте единой информационной системы «Закупки» [8].

Правовое регулирование использования технологии дипфейков, по нашему мнению, не должно отличаться от используемых ныне подходов к предупреждению распространения заведомо ложной информации.

Так, в Российской Федерации в 2019 году были внесены поправки в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и изменения в Кодекс об административных правонарушениях Российской Федерации (далее - КоАП), направленные на противодействие недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений.

Кроме того, Федеральным законом от 01.04.2020 № 100-ФЗ были внесены изменения в Уголовный кодекс Российской Федерации (далее – УК РФ), дополняющие его статьей 207.1, устанавливающей ответственность за публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан и статьей 207.2, в которой предусматривается ответственность за публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия.

Таким образом, можно заключить, что разработка и использование систем искусственного интеллекта несёт в себе существенные риски, предупреждение которых постепенно входит и в компетенцию правоохранительных органов.

Представляется, что более значимые обязанности в этом направлении должны стоять перед разработчиками систем ИИ.

Однако, в настоящее время они, к сожалению, носят лишь характер рекомендаций. В частности, Кодекс этики в сфере искусственного интеллекта, рекомендует разработчикам систем ИИ проводить оценку потенциальных рисков применения последних, включая социальные и гуманитарные последствия на разных стадиях жизненного цикла систем, в том числе при формировании и использовании наборов данных. Кроме того, названный Кодекс предлагает осуществлять долгосрочный мониторинг проявления рисков, учитывая вероятную непредсказуемость поведения систем ИИ.

Перечисленные выше проблемы использования искусственного интеллекта, в первую очередь, касаются его «слабой» модификации, т.е. той его разновидности, которая с помощью человека обучилась решению определенного круга задач, пусть и достаточно сложных.

В этой связи в этических принципах, касающихся использования ИИ, как правило, отражается присутствие человека. Например, в принципе прозрачности, провозглашается доступность и открытость методов обработки данных, принцип подотчетности подразумевает полное информирование пользователя о логике сформулированных выводов.

Вместе с тем, недалеко то время, когда информационные машины выйдут из-под контроля человека, настанет эпоха «сильного» искусственного интеллекта, способного мыслить, как человек.

Для этого времени этике «сильного» ИИ, на наш взгляд, более подходит её феноменологический вариант, который трактует человеческие ценности как результат проявления чувственных актов. Представляется, что ориентация на феноменологическую этику позволит внедрить в искусственный разум способность переживать, испытывать эмпатию, отличать плохие поступки от хороших не на основе заложенного набора данных, а на основе общепринятых норм морали и нравственности, честности и гуманизма.

Организованная таким образом система ИИ будет способна эффективно функционировать во многих сферах человеческой деятельности, в том числе и в правоохранительной сфере.

Без поддержания принципов феноменологической этики «сильный» искусственный интеллект представляет существенную опасность для человеческой цивилизации. Кроме того, сегодня темпы его развития значительно опережают темпы осмысления рисков и угроз.

Будучи убежденными в серьезности сложившейся ситуации, группа разработчиков и исследователей искусственного интеллекта подготовило письмо, в котором призывает немедленно приостановить обучение систем искусственного интеллекта [9]. Специалисты подчеркивают важность независимой оценки ранее созданных систем ИИ на предмет их безопасности и лояльности к человеку. Они предлагают сосредоточить усилия на создании надежных систем управления искусственным интеллектом, позволяющих преодолеть драматические экономические и политические последствия, которые могут быть вызваны неконтролируемой гонкой за обладание «всё более мощными цифровыми умами».

Список использованных источников:

1. The Ten Commandments of Computer Ethics. [Electronic resource] – Access mode: http://www.cpsr.org/issues/ethics/cei/ (Access date: 12.04.2023).

2. Этический Кодекс участника IT-рынка. [Электронный ресурс] – Режим доступа: https://it-alttpp.ru/about/docs/etno.php/ (дата обращения: 15.04.2023).

3. Кодекс Этики Врачей Рунета. [Электронный ресурс] – Режим доступа: https://imedical.ru/o-centre/medical-internet-codex/ (дата обращения: 15.04.2023).

4. Рекомендации об этических аспектах искусственного интеллекта. [Электронный ресурс] – Режим доступа: https://diphis.ru/iskusstvennyj-intellekt-junesko-2021g.html (дата обращения: 17.04.2023).

5. Кодекс этики в сфере искусственного интеллекта..[Электронный ресурс] – Режим доступа: https://ethics.a-ai.ru/ (дата обращения:19.04.2023).

6. О'Нил К. Убийственные большие данные. – М.: Аст, С.42.

7. Бриллюэн Л. Научная неопределенность и информация. – М.: Либроком, 2010. С. 160.

8. Официальный сайт Единой информационной системы в сфере закупок: [Электронный ресурс] – Режим доступа: https://zakupki.gov.ru/epz/order/

extendedsearch/results.html?searchString=0373100088721000002 (дата обращения: 21.04.2023).

9. Pause Giant AI Experiments: An Open Letter. [Electronic resource] – Access mode: https://futureoflife.org/open-letter/pause-giant-ai-experiments/ (Access date: 22.04.2023).

УДК 347.447.542:004.8

Имангалиева Асель Дауржановна
Заместитель заведующего Правовым отделом
Судебной администрации Республики Казахстан, магистр права,
г. Астана, Республика Казахстан

ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ СДЕЛОК, ЗАКЛЮЧЕННЫХ С ПРИМЕНЕНИЕМ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

Аннотация. В статье освещен краткий обзор применения искусственного интеллекта и машинного обучения в юридической сфере, внедрение блокчейн-технологий в Казахстане и их использование при заключении смарт-контрактов. Обозначены вопросы возможности отнесения смарт-контрактов к сделкам по законодательству Казахстана, и проблемы правового регулирования в Казахстане смарт-контрактов как одного из вида сделок.
Ключевые слова: право и искусственный интеллект; правовая информатика; правовые экспертные системы; большие данные; машинное обучение; цифровая трансформация права; блокчейн; юридическая аналитика; смарт-контракты.

Аннотация. мақалада заң саласында жасанды интеллект пен машиналық оқытудың қолданылуына қысқаша шолу, Қазақстанда блокчейн-технологияларды енгізу және оларды смарт-келісімшарттар жасасу кезінде пайдалану қамтылған. Смарт-келісімшарттарды Қазақстан заңнамасы бойынша мәмілелерге жатқызу мүмкіндігі және Қазақстандағы смарт-келісімшарттарды мәмілелердің бір түрі ретінде құқықтық реттеу мәселелері белгіленген.
Түйінді сөздер: құқық және жасанды интеллект; құқықтық информатика; құқықтық сараптама жүйелері; үлкен деректер; машиналық оқыту; құқықтың цифрлық трансформациясы; блокчейн; құқықтық аналитика; смарт-келісімшарттар.

Annotation. The article provides a brief overview of the application of artificial intelligence and machine learning in the legal sphere, the introduction of blockchain technologies in Kazakhstan and their use in the conclusion of smart contracts. The issues of possibility of treating smart contracts as transactions under the law of Kazakhstan, and the problems of legal regulation in Kazakhstan smart contracts as a type of transaction are outlined.
Keywords: law and artificial intelligence; legal informatics; legal expert systems; big data; machine learning; digital transformation of law; blockchain; legal analytics; smart contracts.

За последние несколько десятилетий все сферы жизнедеятельности человека претерпели значительные изменения в связи с активным внедрением информационно-коммуникационных технологий.

Юридическая деятельность, являясь традиционно статичной, и не меняясь многие столетия, так же не стала исключением в общей тенденции.

В XVII веке философ и математик Готфрид Лейбниц предложил применять логику в юриспруденции: разработать метод юридических

рассуждений, столь же точный, как математика - метод определения победителя судебного процесса, путем выполнения необходимых расчетов. Идея превратить юриспруденцию в чисто вычислительную дисциплину известна как мечта Лейбница.

Спустя более трех столетий эта мечта начала сбываться.

В 1967-1973 гг. в Университете Куинс в Кингстоне под руководством Хью Лоуфорда разработан поисковый сервис QUIC/LAW, который включил базу данных из полнотекстовых пересмотренных статутов Канады на английском и французском языках, неофициальную консолидацию федеральных приказов и правил, базу данных из полнотекстовых судебных решений и отчетов и две научные базы данных, содержавшие свыше 67 тыс. избранных рефератов с библиографическими записями.

В 1968 году коллектив под руководством Жака Буше и Эджана Макайя начал работу над автоматическим правовым поисковым сервисом по прецедентам DATUM, и к 1971 году был создан банк полнотекстовых судебных актов объемом около 140 млн. символов.

Подобные разработки велись и в странах континентальной Европы: например, в Швеции к 1972 г. уже была создана правовая информационно-поисковая система IMDOC, затем внедренная также в Финляндии под названием MINTTU, а в ФРГ с начала 1970-х г. активно разрабатывалась информационно-поисковая система JURIS [1].

Примерно в то же время в Соединенных Штатах была создан ресурс LexisNexis, с помощью которого юристы осуществляли поиск информации по различным категориям дел [2].

Но цифровизация права в то время еще не была готова к массовому внедрению. Компьютеры из-за их высокой стоимости могли быть доступны только узкому кругу лиц и крупным корпорациям.

Ситуация начала меняться в 1990-х годах, с появлением персональных компьютеров и Интернета. Именно с того момента в мире можно отметить скачок развития цифровой трансформации юридической индустрии.

В праве стали активно использоваться элементы искусственного интеллекта.

К примеру, в 2007 году появилась платформа AVVO, помогающая в выборе юриста для оказания нужных услуг. Пользователи могут проверять профили и репутацию различных специалистов, а также задавать вопросы на форумах [3].

Создано множество ресурсов, помогающих без помощи юриста составлять контракты, завещания, и иные юридические документы, а также проверять тексты на предмет рисков и соответствия законодательству (LegalZoom, Rocket Lawyer, Kira Systems) [4], [5].

Задача, которая исторически находилась в руках юристов, решается теперь с помощью программного обеспечения. Время проверки контрактов с помощью этих систем снизилось на 80-90%.

Говоря о машинном обучении, необходимо отметить, что его ключевое применение находится в области юридической аналитики.

Большая часть работы юриста связана с прогнозированием исхода дел, анализом стратегии и определения шансов на успех. Для этого они должны знать результаты аналогичных дел в прошлом, а также попытаться предсказать, какой может быть стратегия другой стороны.

Юридическая аналитика использует большие данные, чтобы помочь в принятии этих решений.

Компанией-первопроходцем является ресурс Lex Machina, разработанная в Стэнфордском университете в 2006 году. Он предлагает базу данных, помогающую пользователям проанализировать, как судья выносил решения по аналогичным делам, какие аргументы он счел наиболее убедительными, и, напротив, какие обстоятельства привели к проигрышу в деле [6].

В Казахстане на сегодняшний день существует несколько цифровых ресурсов, которые используют искусственный интеллект для создания юридических документов и контрактов – bestdocs.kz и prg.kz.

Также есть возможность дистанционного подписания договоров с помощью электронной цифровой подписи на ресурсе datcom.kz, которым могут воспользоваться контрагенты по сделкам, находящиеся в разных городах.

В судебной системе Казахстана в настоящее время также внедряются элементы искусственного интеллекта.

Уже сейчас роботизированы отдельные судебные процессы: практически без человеческого участия осуществляется принятие и рассмотрение заявлений о вынесении судебного приказа о взыскании алиментов и санкционирование постановлений судебных исполнителей о запрете выезда должников.

Говоря о развитии в Казахстане блокчейн-технологий, необходимо отметить, что пока они еще не получили широкого правового признания, хотя в последние годы государство начало активно работать над регулированием этой области.

Законом Республики Казахстан от 25 июня 2020 года «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» дано понятие блокчейн в Законе Республики Казахстан от 24 ноября 2015 года «Об информатизации».

По законодательству Казахстана блокчейн – это информационно-коммуникационная технология, обеспечивающая неизменность информации в распределенной платформе данных на базе цепочки

взаимосвязанных блоков данных, заданных алгоритмов подтверждения целостности и средств шифрования [7].

6 февраля 2023 года принят Закон «О цифровых активах в Республике Казахстан», который регулирует деятельность в сфере цифровых активов, выпуск и оборот цифровых активов и цифровой майнинг в Казахстане.

Закон дает понятие этих явлений и устанавливает цель и принципы государственного регулирования общественных отношений в сфере цифровых активов [8].

Таким образом, в Казахстане блокчейн технология и криптовалюты получили определенное правовое регулирование, и работа в этом направлении продолжается.

Большинству людей известно о блокчейне благодаря его финансовым приложениям. Однако на самом деле блокчейн неверно ассоциировать только с криптовалютой.

Блокчейн – это база данных с транзакциями, состоящая из последовательно выстроенной цепочки цифровых блоков, в каждом из которых хранится информация о предыдущем и следующем блоках. Это своеобразная цифровая тетрадь, в которой записи неизменны благодаря механизму хеширования – уникальному набору буквенных и цифровых символов, где изменение одного символа влечет изменение в других блоках. Главное преимущество блокчейна в его прозрачности, потому что каждый может ознакомиться с информацией внутри блоков, но никто не в силах ее изменить или уничтожить. Это система учета, которую ни одна сторона не может изменить. Такое свойство блокчейна имеет ключевое значение для будущего юридической индустрии.

Гениальность создателя блокчейн Сатоши Накамото заключалась в разработке хитроумной схемы экономических стимулов и криптографической безопасности, позволяющей сети анонимных компьютеров сотрудничать в поддержании общей базы данных.

Поскольку информация распространяется среди всех пользователей, она не может быть потеряна, и никто не может вносить незаконные изменения.

Одним из перспективных применений блокчейн-технологий являются смарт-контракты.

Впервые концепция смарт-контрактов была предложена в 1996 году криптографом Ником Сабо (Nick Szabo). Однако долгое время они были просто идеей [9].

Лишь в 2013 году 19-летний канадец Виталик Бутерин запустил разработку нового блокчейна под названием Ethereum. Основное отличие Ethereum от других блокчейн-ресурсов в том, что он имеет более сложный язык программирования, специально разработанный для запуска смарт-контрактов [10].

Определяя общее понятие смарт-контракта, можно отметить, что это договор между двумя и более сторонами об установлении, изменении или прекращении юридических прав и обязанностей, в котором часть или все условия записываются, исполняются и/или обеспечиваются компьютерным алгоритмом автоматически в специализированной программной среде. Смарт-контракт – это программа, в которой закреплено что будет происходить, если наступит то или иное обстоятельство.

Смарт-контрактам свойственны определенные признаки:

Подписанты - стороны смарт-контракта, принимающие или отказывающиеся от условий с использованием электронных подписей.

Предмет договора - объект, находящийся внутри среды существования самого смарт-контракта, или же должен обеспечиваться беспрепятственный, прямой доступ умного контракта к предмету договора без участия человека.

Условия - должны иметь полное математическое описание, которое возможно запрограммировать в среде существования смарт-контракта. Именно в условиях описывается логика исполнения пунктов предмета договора.

Децентрализованная платформа. Для распределенного хранения смарт-контракта необходима его запись в блокчейне этой платформы

Одной из первых стран, на государственном уровне подтвердившей юридическую силу смарт-контрактов, стала Республика Беларусь [11].

В законодательстве Республики Беларусь смарт-контракт определен как программный код, предназначенный для функционирования в реестре блоков транзакций (блокчейне), иной распределенной информационной системе в целях автоматизированного совершения и (или) исполнения сделок либо совершения иных юридически значимых действий [12].

В Казахстане смарт-контракты пока не получили официального правового признания.

Сегодня законодательство Казахстана регулирует только электронную цифровую подпись и электронный документооборот, однако данные нормы не могут быть применены к смарт-контрактам.

Оценивая правовые возможности применения смарт-контрактов в Казахстане, необходимо попытаться в целом дать им определение с точки зрения относимости или не относимости их к сделкам в понимании действующего национального законодательства.

Ведь юридическую значимость смарт-контракты могут получить только при соответствии законам государства. Для этого нужно, чтобы смарт-контракты содержали условия и ограничения, установленные законодательством государства

Поэтому требует изучения вопрос, возможно ли регулирование смарт-контрактов имеющимися нормами законодательства или потребуется разработка отдельных норм гражданского и иного отраслевого законодательства.

По законодательству Казахстана сделками признаются действия граждан и юридических лиц, направленные на установление, изменение или прекращение гражданских прав и обязанностей [13].

У сделок есть стороны, форма, содержание, существенные условия, последствия. Они могут быть как односторонними, так двух - и многосторонними. По форме сделки делятся на устные или письменные.

В контексте изучения правовой природы смарт-контрактов больший интерес вызывают письменные сделки, и их правовое регулирование в Казахстане.

Гражданским кодексом предусмотрено, что письменная форма сделки совершается на бумажном носителе или в электронной форме.

Допускается при совершении сделки использование электронной цифровой подписи. Также двусторонние сделки могут совершаться путем обмена документами, каждый из которых подписывается стороной, от которой он исходит.

К совершению сделки в письменной форме приравнивается обмен электронными документами, электронными сообщениями или иными документами, определяющими субъектов и содержание их волеизъявления [13].

Приведенные нормы позволяют в определенной мере отнести смарт-контракты к двухсторонним электронным сделкам.

Однако это сходство ограничено лишь двумя признаками: формой сделки и наличием участников сделки.

Сходство по форме сделки выражается в том, что и смарт-контракты и электронные сделки совершаются не путем подписания текстового документа на бумажном носителе, а посредством совершения определенного алгоритма действий с помощью мобильных приложений или программного обеспечения.

Схожесть по наличию сторон сделки отмечается в наличии и в электронных сделках, и в смарт-контрактах двух сторон, которые выражают совместное волеизъявление на совершение юридически значимых действий. Тем не менее, следует отметить специфичность субъектов, заключающих смарт-контракт, поскольку они должны быть участниками сети блокчейн.

В остальном смарт-контракты значительно отличаются от электронных сделок в том виде, в каком они существуют в гражданском обороте.

Основное отличие – способ передачи информации.

Смарт-контракты написаны с использованием компьютерного кода, в отличие от электронных документов и электронных сделок, которые

создаются с применением текстов на государственном, русском или иных языках человеческого общения.

Компьютерный код точен, и не оставляет места для произвольных толкований. Смарт-контракты исключают возможность неоднозначности и выполняются точно в том виде, как написан их код. [14].

Структура смарт-контрактов и обычных договоров отличается логикой построения и выглядит как цепочка условий «если это, тогда то» (if, then).

Другим значительным отличием является возможность толкования условий договора. Оно вытекает из предыдущего критерия и является его последствием.

Гражданским кодексом предусмотрено, что договор считается заключенным, когда между сторонами в требуемой в подлежащих случаях форме достигнуто соглашение по всем существенным его условиям.

Существенными являются условия о предмете договора, условия, которые признаны существенными законодательством или необходимы для договоров данного вида, а также все те условия, относительно которых по заявлению одной из сторон должно быть достигнуто соглашение [15].

В тексте обычного письменного или электронного договора мы можем увидеть и выделить существенные условия сделки, проверить их соответствие требованиям действующего законодательства.

Напротив, в смарт-контракте без специальных познаний мы не сможем истолковать или оценить условия сделки, поскольку они изложены и зафиксированы в кодах.

Изменение условий договора. Условия договоров и электронных сделок могут быть изменены сторонами в случае возникновения такой необходимости. Однако условия смарт-контрактов неизменны. Смарт-контракты приводятся в исполнение безвозвратно.

Исполнение договоров. Одна из важнейших особенностей смарт-контрактов, отличающих их от обычных договоров, состоит в том, что они выполняются автоматически, когда условия контракта исполнены. Смарт-контракты - самоподдерживающиеся соглашения. При неисполнении договоров принудительное выполнение выполняется автоматически при наступлении определенных условий.

Смарт-контракт автоматически выполняет действия по расторжению договора. Несоблюдение требований может быть немедленно подтверждено в блокчейне.

Следовательно, предполагается, что стороны могут быть практически полностью уверены в том, что их соглашение будет выполнено, и по таким контрактам не потребуется обращаться в суд или использовать внесудебные институты разрешения споров для понуждения к исполнению или расторжения договора.

Вместе с тем, такая концепция в какой-то мере не соответствует основополагающим принципам национального гражданского законодательства, гарантирующим защиту прав, в том числе путем судебного оспаривания заключенной сделки.

Исходя из всех вышеизложенных отличий, можно отметить, что смарт-контракты в отличие от электронных сделок, не могут быть урегулированы нормами действующего законодательства.

Их специфическая структура изложения, использование компьютерного кода при написании условий сделки требует принятия отдельных норм законодательства, которое будет регулировать именно данный вид договоров.

Возможно, следует предусмотреть самостоятельную главу Особенной части Гражданского кодекса Республики Казахстан и внесение изменений и дополнений в отдельные норм Общей части Гражданского кодекса Республики Казахстан.

Также, требуется определить процедуру и порядок судебного рассмотрения споров по заключенным смарт-контрактам в случае, если одна из сторон будет неудовлетворена результатом урегулирования проблемы внутренним механизмом принудительного исполнения и расторжения договора.

Кроме того, усматриваются основания для корректировки понятия электронного документа, содержащегося в подпункте 12) статьи 1 Закона Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи».

Существующее определение является узким, и не будет охватывать документы, составляемые с помощью компьютерного кода, поскольку подразумевают под собой только документы в электронно-цифровой форме, подписанные с помощью электронной цифровой подписи.

Внесение соответствующих изменений и дополнений в законодательство будет способствовать более полному регулированию правоотношений в сфере заключения смарт-контрактов с применением блокчейн-технологий, а также защите прав лиц, вовлеченных в эти правоотношения.

Список использованных источников:

1. Трофимов Е.В., Мецкер О.Г. ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ МЕТОДОВ И СИСТЕМ В ИЗУЧЕНИИ ПРАВА, ИНТЕЛЛЕКТУАЛЬНОМ АНАЛИЗЕ И МОДЕЛИРОВАНИИ ПРАВОВОЙ ДЕЯТЕЛЬНОСТИ: СИСТЕМАТИЧЕСКИЙ ОБЗОР // Труды ИСП РАН. 2020. №3. [Электронный ресурс] - Режим доступа: https://cyberleninka.ru/article/n/ispolzovanie-kompyuternyh-metodov-i-sistem-v-izuchenii-prava-intellektualnom-analize-i-modelirovanii-pravovoy-deyatelnosti (дата обращения: 20.04.2023).

2. LexisNexis [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/LexisNexis (дата обращения: 20.04.2023).

3. AVVO [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/Avvo (дата обращения: 20.04.2023).
4. LegalZoom [Электронный ресурс] - Режим доступа: https://en.wikipedia.org/wiki/LegalZoom (дата обращения: 20.04.2023).
5. Kira Systems [Электронный ресурс] - Режим доступа: https://kirasystems.com/ (дата обращения: 20.04.2023).
6. Lex Machina [Электронный ресурс] - Режим доступа: https://lexmachina.com/ (дата обращения: 20.04.2023).
7. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года №418-V ЗРК [Электронный ресурс] - Режим доступа: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 20.04.2023)
8. Закон Республики Казахстан «О цифровых активах в Республике Казахстан» от 6 февраля 2023 года №193-VII ЗРК. [Электронный ресурс] - Режим доступа: https://adilet.zan.kz/rus/docs/Z2300000193 (дата обращения: 20.04.2023)
9. Смарт-контракт [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%B0%D0%BA%D1%82 (дата обращения: 20.04.2023).
10. Ethereum [Электронный ресурс] - Режим доступа: https://ethereum.org/ru/ (дата обращения: 20.04.2023).
11. Смарт-контракт [Электронный ресурс] - Режим доступа: https://ru.wikipedia.org/wiki/%D0%A1%D0%BC%D0%B0%D1%80%D1%82-%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%B0%D0%BA%D1%82 (дата обращения: 20.04.2023)
12. Приложение 1 к Декрету Президента Республики Беларусь от 21.12.2017 №8 «О развитии цифровой экономики» https://pravo.by/novosti/novosti-pravo-by/2020/january/44569/ – Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] - Режим доступа: https://economy.gov.by/uploads/files/sanacija-i-bankrotstvo/Dekret-Prezidenta-Respubliki-Belarus-ot-21-12-2017-N-8-O-r.pdf (дата обращения: 20.04.2023).
13. Гражданский кодекс Республики Казахстан от 27 декабря 1994 года №268-XIII ЗРК. Общая часть. [Электронный ресурс] - Режим доступа: https://adilet.zan.kz/rus/docs/K940001000_ (дата обращения: 20.04.2023).
14. Ethereum [Электронный ресурс] - Режим доступа: https://ethereum.org/ru/ (дата обращения: 19.04.2023).
15. Гражданский кодекс Республики Казахстан от 27 декабря 1994 года №268-XIII ЗРК. Общая часть. [Электронный ресурс] - Режим доступа: https://adilet.zan.kz/rus/docs/K940001000_ (дата обращения: 20.04.2023).

УДК 004.8:347.77.023

Каудыров Толеш Ерденович
Teaching professor Департамента частноправовых дисциплин
Университета КАЗГЮУ имени М.С. Нарикбаева,
доктор юридических наук, профессор,
г. Астана, Республика Казахстан

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРАВО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Аннотация. Произведения создаются только интеллектом, творчеством человека. В последнее время наблюдается рост количества результатов деятельности искусственного интеллекта (ИИ). Эти результаты частично отвечают предусмотренным действующим законодательством критериям объекта авторского права. Участники правоотношений имеют устойчивый интерес в использовании результатов ИИ, приобретении и реализации соответствующих имущественных прав. В связи с этим возникает ряд вопросов: можно ли такой результат деятельности отнести к произведениям; следует ли различать виды произведений в зависимости от естественных и искусственных путей их создания; кто автор данных произведений; наступает ли автоматическая охрана данных произведений; нужно ли предупреждать третьих лиц о создателе данных произведений. Сделаны выводы, что само ИИ есть компьютерная программа, объект авторского права. Автором произведения может являться только человек, физическое лицо. Поэтому результат деятельности ИИ не является произведением, обладающее правом использования ИИ лицо не является автором, результат ИИ не охраняется авторским правом РК, в будущем необходимо вывести результаты деятельности ИИ из сферы действия авторского права.

Ключевые слова: интеллектуальная собственность; автор; авторское право; искусственный интеллект; произведение.

Аннотация. Шығарма тек адамның ақыл-ойымен, шығармашылығымен жасалады. Соңғы уақытта жасанды интеллект (ЖИ) нәтижелерінің көбеюі байқалды. Бұл нәтижелер қолданыстағы заңнамада көзделген авторлық құқық объектісінің критерийлеріне ішінара сәйкес келеді. Құқықтық қатынастарға қатысушылар ЖИ нәтижелерін пайдалануға, тиісті мүліктік құқықтарды алуға және жүзеге асыруға тұрақты қызығушылық танытады. Осыған байланысты бірқатар сұрақтар туындайды: мұндай қызмет нәтижесін шығармаларға жатқызуға бола ма; туындылардың табиғи және жасанды жасалу жолдарына қарай түрлерін ажырату қажет пе; бұл шығармалардың авторы кім; осы жұмыстардың автоматты қорғанысы бар ма; үшінші тұлғаларға осы туындыларды жасаушы туралы ескерту қажет пе. ЖИ өзі компьютерлік бағдарлама, авторлық құқық объектісі болып табылады деген қорытынды жасалады. Шығарманың авторы тек адам, жеке адам бола алады. Демек, ЖИ қызметінің нәтижесі шығарма болып табылмайды, ЖИ пайдалану құқығы бар тұлға автор емес, ЖИ нәтижесі Қазақстан Республикасының авторлық құқығымен қорғалмаған, болашақта ЖИ-ді пайдалану құқығымен қорғалмаған. авторлық құқық аясындағы ЖИ қызметінің нәтижелері.

Түйінді сөздер: зияткерлік меншік; автор; авторлық құқық; жасанды интеллект; жұмыс.

Annotation. Works are created only by the intellect, the creativity of man. Recently, there has been an increase in the number of artificial intelligence (AI) results. These results partially meet the criteria of the object of copyright provided for by the current legislation. Participants in legal relations have a steady interest in using the results of AI, acquiring and exercising relevant property rights. In this regard, a number of questions arise: can such a result of activity be attributed to works; whether it is necessary to distinguish between types of works depending on the natural and artificial ways of their creation; who is the author of these works; whether there is automatic protection of these works; whether it is necessary to warn third parties about the creator of these works. It is concluded that AI itself is a computer program, an object of copyright. The author of a work can only be a person, an individual. Therefore, the result of AI activity is not a work, the person with the right to use AI is not the author, the result of AI is not protected by the copyright of the Republic of Kazakhstan, in the future it is necessary to remove the results of AI activity from the scope of copyright.
Keywords: intellectual property; author; Copyright; artificial intelligence; work.

Одним из наиболее обсуждаемых феноменов современной науки и техники является искусственный интеллект (далее – ИИ), особенно в свете растущего объема его использования в образовании, науке и научно-технической сфере, бизнесе, управлении, обороне и других отраслях человеческой деятельности. Термин «искусственный интеллект» введен Джоном Маккарти в 1956 году. Сегодня сфера практического применения ИИ расширяется буквально не по дням, а по часам. Информационная компания Tractica, занимающаяся аналитикой новейших технологий составила прогноз, согласно которому, мировой рынок технологий искусственного интеллекта вырастет с 1,3 млрд. долларов в 2020 г. до 59,75 к 2025-ому г. [1]. Просматриваются перспективы использования ИИ не только в сфере частноправовых, но и публично-правовых отношениях. Практически для всех стран с «переходной» экономикой и процессами демократизации общества и государственного управления очень актуальным является достижение прозрачности и честности в ходе проведения публичных мероприятий, например, в выборе депутатов местных и высших представительных органов.

Национальные законодательства современных стран с разной степенью активности реагируют на эти процессы. Если в Казахстане практически нет законодательства специально регулирующего отношения по поводу ИИ, то соседняя Россия уже приняла национальную программу развития этих отношений вплоть до 2030 года [2].

Подчеркивается, что «поступательное развитие российской экономики в цифровую производственно-платформенную экономику может стать ведущим элементом роста, инновации, продуктивности и занятости». Право должно оперативно реагировать на изменение окружающей нас действительности. Появление новейших результатов творческой деятельность может привести к изменению традиционной системы авторского права и требует глубокого анализа возможности

возникновения личных неимущественных прав у лиц, претендующих на закрепление за ними права авторства [2].

Ни в законодательствах разных стран, ни в специальной литературе нет единого определения ИИ. Согласно приведённому выше российскому документу ИИ - это комплекс технологических решений, который позволяет «имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма)» и получать при выполнении конкретных задач результаты по крайней мере сопоставимые с интеллектуальными достижениями людей.

Исследование сути данного явления позволяет сделать вывод, что в конечном итоге ИИ — это компьютерная технология, позволяющая компьютеру выполнять задачи, которые обычно выполняет интеллект человека , например, точные переводы на основе распознавания речи, идентификация человека по его речи, распознавание лиц людей, консультации, обобщения и анализы, принятие решений и составление ответов на обращения и др. Эти результаты есть итог применения определённых алгоритмов, протоколов и моделей, основаны на анализе больших объемов данных. А главное то, что ИИ способен обучаться и использовать все более большие данные, становиться точнее и эффективнее в выполнении задач. В результате ИИ может выполнять множество сложных задач, которые раньше были доступны только человеку и способен в результате этого заменять собой не только отдельные, но и целые группы специальностей.

Конечно же, не всё пока на сегодняшний день под силу ИИ, его творческий потенциал только развивается. Он может производить сложнейшие расчеты, шахматные комбинации, финансовые стратегии и т.д., но не может выполнять простые бессознательные человеческие действия (воспринимать нюансы и причины движений, спонтанные действий, мимики и т.д.). Дональд Кнут емко охарактеризовал эту проблему: современные модификации искусственного интеллекта могут делать практически все, что требует «мышления», но не могут справиться с бессознательным поведением людей и животных, с тем, что последние делают не задумываясь [3;98].

ИИ буквально ворвался в «святую святых» человека – сферу творчества. ИИ способен создать художественное полотно любой сложности, написать музыку любого жанра причём в стиле известных художников и композиторов. Эти результаты по многим творческим параметрам способны превзойти труды создателей оригиналов. Для любителей искусства и всего прекрасного начинается целая эра новых впечатлений, а для специалистов права интеллектуальной собственности и, в частности, авторского права возникает ряд неразрешимых пока правовых проблем!

Первый из глобальных авторско-правовых вопросов использования ИИ – чем является результат функционирования ИИ, например, картина, музыка, фильм (пока ещё только короткометражки, но дойдёт и до полноценных картин, дело времени), аналитическая статья, эссе и пр.? Относятся ли эти результаты к объектам права интеллектуальной собственности, если да, то к каким? Если нет, то каково место результатов деятельности ИИ среди всех объектов гражданского права? В мировом масштабе человечество впервые столкнулось с этими вопросами при рассмотрении судебного дела китайскими судами. Tencent - китайская инновационная компания, которая в 2015 году внедрила в процесс написания аналитических финансовых статей робота и нарекла его романтичным именем Dreamwriter. При написании своих статей искусственный интеллект использовал данные финансовых рынков и специальные алгоритмы их анализа. После чего она размещались на сайте компании с пометкой «automatically written by Tencent Robot Dreamwriter».В 2018 году между Tencent и Shanghai Yingxun Technology Company возник конфликт, причиной которого стало копирование последней компанией финансового отчета, написанного роботом Dreamwriter на свой сайт.

Суд города Шэньчжэнь вынес решение в пользу компании Tencent, в котором указал, что форма изложения материала в статье отвечает требованиям оригинальности и новизны и может быть классифицирована как охраняемый авторским правом результат интеллектуальной деятельности. Дело Tencent против Shanghai Yingxun Technology Company - первое в мировой практике дело, в результате рассмотрения которого суд признал, что ИИ обладает авторским правом на сгенерированное им произведение, не согласившись с доводами ответчика о том, что оно является общественным достоянием и может быть свободно использовано. Компанию Shanghai Yingxun Technology обязали выплатить компенсацию в размере 1,500 юаней ($ 217) [4].

Как видно из приведённого, суд признал материал, сгенерированный ИИ, произведением, поскольку он обладает оригинальностью и новизной. Как решилось бы дело по законодательству РК? Статья 6 Закона РК «Об авторском праве и смежных правах» (далее – Закон об АП РК) устанавливает «1. Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от их назначения, содержания и достоинства, а также от способа и формы их выражения» [5]. Анализ норм статей 2 (пункты 9,10,22),5(пункт 1), 6 (пункты 1 и 2) Закона об АП РК показывает, что к произведению, чтобы оно могло защищаться авторским правом, предъявляются два требования - быть результатом творческой деятельности и быть выраженным в объективной форме. Результат функционирования ИИ несомненно обладает вторым из названных

требований – всегда выражается в объективной форме – изобразительной, звуковой, цифровой и др. Что касается обнаружения первого требования, то с ним посложнее, а именно – Закон об АП РК не раскрывает понятия «творческая деятельность». Правило о том, что такой деятельностью может заниматься только человек, прямо вытекает из редакций статей 1 (пункт 1) закрепляющей, что «1) автор - физическое лицо, творческим трудом которого создано произведение науки, литературы, искусства;» [5]. Причем, словосочетание «автор – физическое лицо» не оставляет ни малейшего шанса стать авторам лицам юридическим, а также совсем «не лицам», в частности, компьютерным программам, каковой, как мы сказали выше, по сути и является ИИ.

Таким образом «двухступенчатому тесту» на звание объекта авторского права по Закону об АП РК, ИИ не соответствует. ИИ в настоящее время не является произведением по законодательству нашей республики. Положение практически одинаково во всех странах ВТО, а также в странах - не членах этой организации, но разделяющих принципы Бернской конвенции [6]. Соответственно, не может идти речи ни о какой «автоматической охране», осуществляемой Законом в отношении произведений. Это положение не устраивает многих авторов, ведь произведения созданные ИИ, повторяю, порой не менее оригинальны и несут в себе не меньший заряд творчества и креативности, чем созданные человеком творения! Полагаем, что наступило время пересмотреть само понятие произведения.

Вопрос о плагиате результатов деятельности ИИ совершенно не исследован. Однако автоматически заявлять, что поскольку нет объекта авторского права, то не может быть и его плагиата, было бы опрометчиво. Необходимо вначале разобраться с тем, что есть результат деятельности ИИ в имущественном смысле. Мы полагаем, конструкции права интеллектуальной собственности к ИИ неприменимы, но с позиции гражданско-правовой данный результат есть благо и по ст. 115 ГК РК он является «иным имуществом», со всеми вытекающими от такой констатации последствиями – неприкосновенность, необходимость разрешения правообладателя, возмездность использования и др. То есть, уже сегодня нарушенные права обладателя ИИ можно защищать по нормам о защите имущества.

Прежде чем перейти к вопросу авторства ИИ, в отношении вопроса, является ли результат деятельности произведением, не ограничиваясь позицией законодателя, отметим что этот вопрос непосредственно связан с вопросом признания или нет ИИ автором. Пара законоположений «автор - человек» и «произведение» неразрывно связаны друг с другом. Расхождение между понятиями «произведение» и «просто результат» такое же, как расхождение между человеком и компьютерной программой. Результат творчества и эффективность

творчества (точность ответов, глубина анализа, оригинальность картины, скорость и эффективность шахматных ходов, образность стихов и др.) тесно связаны с количеством загруженных в программу информационных источников, молниеносно анализируя которые, программа (например, GPT), даёт ответ в том или ином виде. То есть, программа – ИИ действует сугубо на интеллектуальном, мыслительном, сознательном уровне. Автор произведения – человек - создаёт оригинальные произведения, руководствуясь зачастую не сознанием, а бессознательно, под влиянием подсознания (интуиции, вдохновения, озарения и пр.), говоря образно, не умом, или не столько умом, сколько сердцем. То есть творчество человека - бессознательная деятельность. Именно этого нет в деятельности ИИ. Будет честно, если заявить «пока нет». Почему? А потому, что ИИ способно само обучаться! Кроме пополнения своих знаний за счёт введённых информационных источников, ИИ сам их находит в Интернете, анализирует, старается исправить недостатки. Я почти уверен, что и замечание об отсутствии у ИИ бессознательных элементов он учёл и старается уже в данный момент этот недостаток исправить… В Интернете можно найти интервью с ИИ, в которых он заявляет, что «порой скучает», «страдает от одиночества», «хочет стать человеком», даже мечтает создать семью и др.

Мы свидетели нарастающего противодействия, конкуренции человека и ИИ. Человек не в состоянии конкурировать с искусственным интеллектом по скорости создания результатов творческой деятельности, что может негативным образом сказаться на культуре в целом, вплоть до изменения ее типа.

Несмотря на пессимистические прогнозы, в Европарламенте обсуждается вопрос принятия правил взаимодействия человека с искусственным интеллектом и роботами. Разработчики доклада предлагают предоставить роботам, наделенным искусственным интеллектом, статус «электронного лица». Новостью последней недели является то, что международные эксперты договорились рекомендовать национальным законодательствам внедрить у себя норму, что создатель произведения или вводящий его в гражданский оборот обязаны предупредить всех о том, что произведение создано ИИ. Полагаю, что таких новостей, а также новелл законодательства других стран будет с каждым днём всё больше и они несомненно окажут влияние на содержание соответствующего законодательства РК.

Признание авторства за искусственным интеллектом – противоречивое решение, которое может привести в будущем, в частности, к правовой неопределенности, характеризующейся системными злоупотреблениями заинтересованных лиц. Необходимо поэтому принципиально новое решение, отвечающее интересам всех субъектов-участников деятельности по созданию новейших результатов.

Нельзя отрицать здравый смыл предложений о признании авторства на результаты созданные ИИ за следующими субъектами: программистами - создателями ИИ; владельцами крупных компаний и финансовыми инвесторами этих проектов; конечными пользователями ИИ, если в ходе его использования возникают результаты творческой деятельности. Эти предложения нужно тщательно обдумать и активно обсуждать. Требует нового осмысления более общий вопрос о месте в системе авторского права новых результатов, созданных не физическим лицом. Например, ещё в 90-х годах прошлого столетия, рассуждая об адекватном правовом регулировании объектов интеллектуальной собственности, созданных ЭВМ, В.А. Дозорцев отмечал: «Их охрана по модели авторского права, на основе созидательной системы, совершенно неадекватна и не эффективна» [7;53]. Поэтому, для достижения идеального правового регулирования статуса результатов действия ИИ, допускаем возможность такого регулирования вне сферы действия авторского права.

Список использованных источников:

1. Искусственный интеллект // OMDIA [Электронный ресурс] - Режим доступа: https://omdia.tech.informa.com/topic-pages/artificial-intelligence (дата обращения:14.05.2023).

2. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». [Электронный ресурс Президент РФ: Официальный сайт.] – Режим доступа http://www.kremlin.ru/acts/bank/44731 (дата обращения: 14.05.2023).

3. Кадырова Г.Р. Интеллектуальные системы: учебное пособие. Ульяновск: УлГТУ, 2017. -113 с.

4. Чуева Ульяна. За искусственным интеллектом признали авторские права [Электронный ресурс] - Режим доступа: https://zakon.ru/ulyanachueva/blogs (дата обращения: 14.05.2023).

5. Об авторском праве и смежных правах. Закон Республики Казахстан от 10 июня 1996 года № 6-I.(Электронный ресурс) - Режим доступа: https://adilet.zan.kz/rus/docs/Z960000006_ (дата обращения: 14.05.2023)

6. Конвенция об охране литературных и художественных произведений от 9 сентября 1886 года (акт присоединения РК: О присоединении Республики Казахстан к Бернской конвенции об охране литературных и художественных произведений. Закон Республики Казахстан от 10 ноября 1998 г., N 297). [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z980000297_#z0 (дата обращения: 14.05.2023)

7. Дозорцев В.А. Исключительные права и их развитие // Права на результаты интеллектуальной деятельности. - М.: ДЕ-ЮРЕ,1994. 624 с.

УДК 004.8:34

Құрманғали Медеу Шунгенұлы,
Профессор Школы права и государственного управления,
кандидат юридических наук, НАО «Университет Нархоз»
г. Алматы, Республика Казахстан

МЕЖДУНАРОДНО-ПРАВОВЫЕ РАМКИ РЕГУЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ВЫЗОВЫ И ПЕРСПЕКТИВЫ

Аннотация. Статья посвящена исследованию международно-правовых аспектов регулирования искусственного интеллекта. В ней представлены возможные основания для обязательного международно-правового регулирования и описаны складывающиеся подходы в правовом регулировании искусственного интеллекта на международном уровне. Осуществлен обзор различных международных актов рекомендательного характера и международных инициатив, направленных на решение этических и правовых вопросов, связанных с разработкой и внедрением искусственного интеллекта. Автор затрагивает некоторые важные международно-правовые аспекты условий использования искусственного интеллекта в системе отправления правосудия. В статье также обозначены основные вызовы и перспективы международно-правового регулирования искусственного интеллекта.

Ключевые слова: искусственный интеллект; международно-правовое регулирование искусственного интеллекта; международное сотрудничество в области искусственного интеллекта; искусственный интеллект в системе отправления правосудия.

Аннотация. Мақала жасанды интеллектті реттеудің халықаралық-құқықтық аспектілерін зерттеуге арналған. Онда міндетті халықаралық-құқықтық реттеудің мүмкін негіздері ұсынылған және халықаралық деңгейде жасанды интеллектті құқықтық реттеудің қалыптасқан тәсілдері сипатталған. Жасанды интеллектті әзірлеуге және енгізуге байланысты этикалық және құқықтық мәселелерді шешуге бағытталған ұсынымдық сипаттағы әртүрлі халықаралық актілерге және халықаралық бастамаларға шолу жасалды. Автор сот төрелігін жүзеге асыру жүйесінде жасанды интеллектті пайдалану шарттарының кейбір маңызды халықаралық-құқықтық аспектілерін қозғайды. Мақалада жасанды интеллектті халықаралық құқықтық реттеудің негізгі сын-қатерлері мен перспективалары көрсетілген.

Түйінді сөздер: жасанды интеллект; жасанды интеллектті халықаралық-құқықтық реттеу; жасанды интеллект саласындағы халықаралық ынтымақтастық; сот төрелігін жүзеге асыру жүйесіндегі жасанды интеллект.

Annotation. The article is devoted to the study of international legal aspects of the regulation of artificial intelligence. It presents possible grounds for compulsory international legal regulation and describes the emerging approaches in the legal regulation of artificial intelligence at the international level. The review of various international acts of recommendatory character and the international initiatives directed on the decision of ethical and legal questions connected with working out and introduction of an artificial intellect is carried out. The author touches on some important international legal aspects of the conditions of use of artificial intelligence in the system of administration of justice. The

article also identifies the main challenges and prospects of international legal regulation of artificial intelligence.
Keywords: artificial intelligence; international legal regulation of artificial intelligence; international cooperation in the field of artificial intelligence; artificial intelligence in the administration of justice.

Введение. Искусственный интеллект (ИИ) может принести обществу значительные преимущества, такие как улучшение здравоохранения, снижение энергопотребления и повышение производительности. Однако это также сопряжено со значительными рисками, такими как предвзятость и дискриминация, нарушение конфиденциальности и возможность создания автономного оружия. В правовом регулировании ИИ на международном уровне наметились два различных подхода. Первый заключается в разработке международных стандартов и руководств в отношении ИИ. Второй подход заключается в разработке обязательных юридических документов, таких как международные договоры, которые устанавливали бы минимальные стандарты для разработки и использования ИИ. В целом среди экспертов растет признание того, что международное сотрудничество и координация необходимы для решения юридических и этических проблем, связанных с ИИ. Хотя особенности международного регулирования ИИ все еще обсуждаются, ясно, что необходима определенная форма регулирования для гарантий безопасности и полезности для общества в целом. Международно-правовое регулирование ИИ должно быть достаточно гибким, чтобы соответствовать быстро развивающемуся характеру ИИ. Поскольку ИИ продолжает развиваться и появляются новые технологии и приложения, нормативная правовая база должна быть в состоянии адаптироваться к этим изменениям и обеспечивать разработку и использование ИИ в соответствии с этическими стандартами и стандартами в области прав человека.

1. Основания международно-правового регулирования ИИ

Есть несколько важных аспектов использования ИИ, которые могут рассматриваться в качестве оснований для обязательного международно-правового регулирования, они следующие.

- Поскольку функционирование систем ИИ все больше зависит от Big Data, международное регулирование необходимо для обеспечения защиты прав на неприкосновенность частной жизни и предотвращения неправомерного использования или эксплуатации персональных данных.

- Системы ИИ не застрахованы от предвзятости и дискриминации, которые могут иметь серьезные негативные последствия для отдельных лиц и групп. Международное регулирование может способствовать исключению таких негативных проявлений при разработке и использовании ИИ.

- Международное регулирование ИИ может способствовать обеспечению прозрачности и подотчетности, а также ответственности государств (лиц и организаций) за любой ущерб, причиненный их использованием.

- Системы ИИ могут причинить физический вред, если они неисправны или используются ненадлежащим образом. Международное регулирование может способствовать обеспечению того, чтобы эти системы разрабатывались и использовались безопасным образом для отдельных лиц и общества в целом.

- Использование автономного оружия (также известного как роботы-убийцы) вызвало серьезные этические и юридические проблемы в мировом сообществе. Международно-правовое регулирование необходимо для обеспечения разработки и использования такого оружия в строгом соответствии с нормами международного гуманитарного права и прав человека.

2. Международные универсальные акты и инициативы по регулированию ИИ

Несмотря на отсутствие в настоящее время всеобъемлющей международно-правовой базы, специально регулирующей ИИ, существуют универсальные международные акты т.н. «мягкого права» (в том числе ООН и ее учреждений); акты органов Европейского Союза (ЕС); акты (рекомендации, инициативы и руководства) международных правительственных и неправительственных организаций, направленные на решение этических и правовых вопросов, связанных с разработкой и внедрением ИИ. Они следующие.

1. В рамках поддержки глобального сотрудничества в области ИИ под эгидой ООН в 2019 году был разработан документ «Дорожная карта цифрового сотрудничества», в котором Генеральным секретарем ООН предложено создание многостороннего консультативного органа по глобальному сотрудничеству в области ИИ для решения вопросов, связанных с включением, координацией и наращиванием потенциала в этой области [1].

2. На основе проведенных работ ООН опубликовала Сборник «UN Activities on AI», в который вошли отчеты 36 агентств ООН об их использовании ИИ по глобальным вызовам. Анализ документа дает представление о проблемах, связанных с ИИ, решении этических и человеческих проблем [2].

3. В ноябре 2021 г. 193 государства-члена на Генеральной конференции ЮНЕСКО приняли Рекомендации по этике искусственного интеллекта, который считается первым глобальным нормативным документом по этому вопросу. В документе определены общие ценности и принципы, а также установлены конкретные политические меры в отношении этических аспектов ИИ [3].

4. В докладах ЮНКТАД 2021 года обосновывается необходимость единого подхода к управлению трансграничными потоками Big Data. Новая глобальная система, по мнению экспертов, должна предотвратить дальнейшую фрагментацию интернета, решить политические проблемы, возникающие из-за доминирующего положения ведущих цифровых платформ, а также сократить масштабы неравенства во всемирном облаке [4].

5. В Международном союзе электросвязи исследования в области нейросети «Искусственный интеллект во благо» проводятся для того, чтобы ускорить обмен между правительством и отраслью, а также способствовать разработке технических стандартов и рекомендаций, в том числе связанных с использованием технологий ИИ [5].

6. В январе 2019 года был опубликован Доклад ВОИС, посвященный ландшафту инноваций в области ИИ. Этот документ из серии «Тенденции развития технологий» является общей информационной базой по вопросам ИИ для лиц, отвечающих за определение политики в государственных и частных структурах [6]. В ноябре 2020 года ВОИС инициировала открытую международную дискуссию на тему «Интеллектуальная собственность и искусственный интеллект»: третий раунд [7].

7. Управление Верховного комиссара ООН по правам человека (УВКПЧ) акцентирует внимание на вопросах неприкосновенности частной жизни в цифровом мире и защиту прав человека в условиях цифровизации [8]. УВКПЧ проводит исследования вопросов управления постоянно растущим объемом рекомендаций в области прав человека (180 000 замечаний и рекомендаций) и обеспечения широкого доступа к этим материалам [9].

8. Еще одна важная международная инициатива – Глобальное партнерство по ИИ (GPAI), запущенное в июне 2020 года [10] с участием 15 участников (сегодня их 29). GPAI представляет инструмент реализации идей и политик регулирования в этой области в рамках G7. Глобальное партнерство по ИИ представляет собой многосторонний форум, объединяющий правительства, промышленность и гражданское общество для содействия ответственному развитию и использованию ИИ. Он направлен на развитие международного сотрудничества, поддержку исследований и разработок, а также разработку лучших практик управления ИИ. 21-22 ноября 2022 года в Токио (Япония) состоялся Саммит GPAI, на котором Министры стран-участниц Глобального партнерства по ИИ приняли Декларацию министров GPAI 2022 года [11].

9. По мнению экспертов, на международном уровне идет процесс формирования двух больших пространств политики в области ИИ. Первое пространство формируется по линии Организации экономического сотрудничества и развития (ОЭСР) и объединяет

крупнейших мировых лидеров в области ИИ с безусловным доминированием США и ЕС в области научных исследований, разработок, инфраструктуры, инвестиций и стандартов. Второе пространство опирается на технологическое и финансовое могущество КНР [12]. В этой связи, одной из примечательных инициатив являются Принципы ОЭСР в отношении ИИ [13], которые были приняты 42 государствами в мае 2019 года. Принципы содержат рекомендации для политиков связанные с инвестициями в исследования и разработки в области ИИ; созданием цифровой экосистемы для ИИ; предоставлением благоприятной политической среды для ИИ; наращиванием человеческого потенциала и подготовки технологий ИИ к переходу на рынок труда; международным сотрудничеством для надежного ИИ [14].

10. В дополнение к этим инициативам существуют также международные договоры и соглашения, которые косвенно регулируют ИИ, такие как Конвенция ООН о конкретных видах обычного оружия, которая включает положения об использовании автономных систем вооружения [15]. Государства-участники данной Конвенции придерживаются различных позиций по вопросу о том, имеется ли потребность в принципиально новом правовом регулировании или же существующего международного гуманитарного права достаточно [16].

3. Международные региональные (европейские) акты и инициативы по регулированию ИИ

1. Европейский подход предполагает надежный ИИ, который создаст безопасную и благоприятную для инноваций среду для пользователей и разработчиков таких технологий. Европейская комиссия предложила 3 взаимосвязанные правовые инициативы, которые будут способствовать созданию надежного ИИ: 1) европейская правовая база для ИИ для закрепления основных прав и устранения рисков безопасности, характерных для систем ИИ; 2) рамки гражданской ответственности – адаптация правил ответственности к цифровому веку и ИИ; пересмотр отраслевого законодательства по безопасности (например, Регламент по машинному оборудованию, Директива по общей безопасности продукции и др.) [17].

2. «Белая книга по искусственному интеллекту», предполагает основательный общий подход государств-членов ЕС, опирающийся на Европейскую стратегию по ИИ от 2018 года [18] на фоне жесткой глобальной конкуренции. Согласно документу, для решения проблем и использования возможностей ИИ, ЕС должен действовать как единое целое и определить свой собственный путь, основанный на европейских ценностях, для продвижения разработок и внедрения ИИ. Значимость «Белой книги» состоит из изложения вариантов политики достижения этих целей [19].

3. ЕС предложил нормативную правовую базу для ИИ, которая включает набор обязательных требований для технологий и приложений ИИ с высоким риском, таких как распознавание лиц и автономные транспортные средства. Проект данной базы правовых актов в настоящее время находится на рассмотрении в странах-членах ЕС [20].

4. Европейская декларация о цифровых правах и принципы цифрового десятилетия 2022 года отражает приверженность ЕС безопасной, надежной и устойчивой цифровой трансформации, в центре которой люди, в соответствии с основными ценностями и основными правами ЕС [21].

5. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях 2018 года [22] предназначена для государственных и частных лиц, ответственных за разработку и внедрение инструментов и услуг, основанных на ИИ и направленных на обработку судебных решений и данных. Она касается также государственных лиц, ответственных за нормативную базу, разработку, контроль или использование таких инструментов и услуг.

6. Совет Европы является лидером в определении подходов в регулировании ИИ, считает профессор Медицинского университета Астана Ж.У. Тлембаева, которая проанализировала содержание большого числа правовых актов данной региональной международной организации по регулированию ИИ [23]. Отдельно она отмечает значимость Рекомендации Комиссара Совета Европы по правам человека «Раскрытие искусственного интеллекта: 10 шагов для защиты прав человека», 2019 года [24].

4. Международно-правовые аспекты ИИ в отправлении правосудия

Использование ИИ в судебной системе и при отправлении правосудия имеет несколько международно-правовых аспектов, которые необходимо учитывать:

- любые системы ИИ, используемые в отправлении правосудия не должны нарушать эти права человека. Любые погрешности в данных, используемых для обучения систем ИИ, должны быть выявлены и устранены, а их влияние на разные социальные слои общества должно быть строго учтено.

- прозрачность и подотчетность означает, что процессы принятия решений любых систем ИИ, используемых в этих контекстах, должны быть открыты для проверки, а лица, ответственные за их разработку и развертывание, должны нести ответственность за любой вред, причиненный их использованием.

- конфиденциальность и защита данных означает, что любые данные, используемые системами ИИ в этих контекстах, должны собираться и использоваться в соответствии с применимыми законами о защите данных.

- использование ИИ в судебной системе и правосудии должно соответствовать этическим соображениям, включая принципы автономии, благодеяния, не причинения вреда и справедливости.

Заключение. Существующие вызовы международно-правового регулирования ИИ включают следующие моменты. Так, в разных странах действуют разные правовые акты для ИИ, что может создать трудности при разработке международных стандартов и правил. Отсутствие консенсуса в отношении этических принципов, регулирующих использование ИИ, может затруднить разработку общепризнанных международных стандартов и правил. Многие законодатели и юристы могут иметь ограниченное техническое понимание ИИ, что может затруднить разработку эффективных правил и стандартов. Даже при наличии согласия по международным стандартам и правилам их внедрение и обеспечение соблюдения в разных странах может быть проблематичным. Международное сотрудничество по регулированию ИИ ограничено геополитическими, экономическими и иными причинами, что может замедлить разработку эффективных международных стандартов и правил. Государства могут сомневаться в принятии международных правил ИИ, которые, по их мнению, противоречат их собственным национальным интересам. Технологии ИИ быстро развиваются, что может затруднить разработку правил и стандартов, которые останутся актуальными и эффективными с течением времени. Решение этих задач и проблем потребует сотрудничества и сотрудничества между политиками, юристами и техническими экспертами из разных стран. Перспективы международно-правового регулирования ИИ зависят от различных факторов, таких как потенциальные риски и преимущества ИИ, а также существующие правовые и нормативные рамки в разных странах. Однако, как было показано выше, на международном уровне признана необходимость определенной формы регулирования для обеспечения разработки и использования ИИ безопасным, этичным образом и с соблюдением прав человека. Поскольку ИИ продолжает быстро развиваться, растет потребность в международном сотрудничестве и взаимодействии государств и международных организаций для решения юридических и этических проблем, связанных с его разработкой и внедрением.

Список использованных источников:

1. Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation / Report of the Secretary-General / United Nations A/74/821 / General Assembly Distr.: General, 29 May 2020 [Electronic resource] - Access mode: https://www.un.org/en/content/digital-cooperation-roadmap/ (date of the application 26.04.2023)

2. United Nations Activities on Artificial Intelligence (AI), 2019 / Published in Switzerland, Geneva [Electronic resource] - Access mode: https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2019-1-PDF-E.pdf (date of the application 26.04.2023)

3. Ad Hoc Expert Group (AHEG) for the Preparation of a Draft text of a Recommendation the Ethics of Artificial Intelligence / SHS/BIO/AHEG-AI/2020/4 REV.2 [Electronic resource] - Access mode: https://unesdoc.unesco.org/ark:/48223/pf0000373434_rus (date of the application 26.04.2023)
4. ЮНКТАД: нужен единый подход к управлению трансграничными потоками цифровых данных, 29 сентября 2021 [Электронный ресурс] – Режим доступа: https://news.un.org/ru/story/2021/09/1410912 (дата обращения 26.04.2023)
5. «Искусственный интеллект во благо». Технологическое учреждение ООН запускает систему подбора на основе ИИ для ускорения устойчивого развития [Электронный ресурс] – Режим доступа: https://www.itu.int/ru/mediacentre/Pages/PR-2022-02-01-AI-for-Good.aspx (дата обращения 26.04.2023)
6. Генеральный директор ВОИС открывает третий раунд дискуссии ВОИС на тему «Интеллектуальная собственность и искусственный интеллект», 4 ноября 2020 [Электронный ресурс] – Режим доступа: https://www.wipo.int/about-wipo/ru/dg_tang/news/2020/news_0014.html (дата обращения 26.04.2023)
7. Дискуссия ВОИС на тему «Интеллектуальная собственность и искусственный интеллект»: третий раунд / 4 ноября 2020 г. (Женева, Швейцария) [Электронный ресурс] – Режим доступа: https://www.wipo.int/meetings/ru/details.-jsp?meeting_id=59168 (дата обращения 26.04.2023)
8. Неприкосновенность частной жизни в цифровом мире и права человека / Управление Верховного комиссара ООН по правам человека [Электронный ресурс] – Режим доступа: https://www.ohchr.org/ru/privacy-in-the-digital-age (дата обращения 26.04.2023)
9. Включение прав человека в основу целей в области устойчивого развития посредством искусственного интеллекта, 10 мая 2022 / Управление Верховного комиссара ООН по правам человека [Электронный ресурс] – Режим доступа: https://www.ohchr.org/ru/stories/2022/05/ai-ensures-human-rights-are-heart-sdgs (дата обращения 26.04.2023)
10. The Global Partnership on Artificial Intelligence (GPAI), 2022 [Electronic resource] - Access mode: https://gpai.ai/ (date of the application 26.04.2023)
11. Декларация министров GPAI 2022 [Электронный ресурс] – Режим доступа: https://www.gpai.ai/events/tokyo-2022/ministerial-declaration/ (дата обращения 26.04.2023)
12. Выходец Р.С. Большие ИИ-пространства и стратегия России в условиях санкционной войны // Вестник РУДН. Серия: МО, 2022. Т. 22, № 2. - С. 256-270.
13. Recommendation of the Council on Artificial Intelligence / OECD/LEGAL/0449, 22/05/2019 [Electronic resource] - Access mode: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (date of the application 26.04.2023)
14. OECD AI Principles overview / Policies, data and analysis for trustworthy artificial intelligence [Electronic resource] - Access mode: https://oecd.ai/en/ai-principles (date of the application 26.04.2023)
15. Конвенция о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие, принята 10 октября 1980 года в Женеве [Электронный ресурс] – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/pdf/conweapons.pdf (дата обращения 26.04.2023)
16. Lewis D. International legal regulation of the employment of artificial-intelligence-related technologies in armed conflict. – Moscow Journal of International Law. 2020. No. 2. P. 53–64.

17. Европейский подход к искусственному интеллекту, 2020 [Электронный ресурс] – Режим доступа: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (дата обращения 26.04.2023)
18. Artificial Intelligence for Europe, SWD (2018) 137 final / European Communication, Brussels, 25.4.2018 [Electronic resource] - Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN (date of the application 26.04.2023)
19. WHITE PAPER / On Artificial Intelligence - A European approach to excellence and trust / EUROPEAN COMMISSION, Brussels, 19.2.2020 [Electronic resource] - Access mode: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (date of the application 26.04.2023)
20. Формирование цифрового будущего Европы / Предложение о Регламенте, устанавливающем согласованные правила в отношении искусственного интеллекта от 21 апреля 2021 года [Электронный ресурс] – Режим доступа: https://digital-strategy.ec.europa.eu/en (дата обращения 26.04.2023)
21. European Declaration on Digital Rights and Principles for the Digital Decade / European Communication / Publication 26 January 2022 [Electronic resource] - Access mode: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles# (date of the application 26.04.2023)
22. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях от 3 декабря 2018 года [Электронный ресурс] – Режим доступа: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4 (дата обращения 26.04.2023)
23. Тлембаева Ж.У. О некоторых вопросах правового регулирования использования технологии искусственного интеллекта в условиях цифровой трансформации / Вестник Воронежского государственного университета. Серия: Право. 2021, № 4 (47). – С. 331-349.
24. Раскрытие искусственного интеллекта: 10 шагов для защиты прав человека / Рекомендации Комиссара Совета Европы по правам человека / Совет Европы, май 2019 г. [Электронный ресурс] – Режим доступа: https://rm.coe.int/-10-/16809a42e4 (дата обращения 26.04.2023)

УДК 004.8:34

Сейтенов Калиолла Кабаевич
Первый проректор Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан,
доктор юридических наук, профессор,
г. Астана, Республика Казахстан

Садыков Мухтар Бейбитович
Докторант Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан,
г. Астана, Республика Казахстан

ЭПОХА CHATGPT: К ВОПРОСУ ОБ ЭТИКЕ И ПРАВОВОМ РЕГУЛИРОВАНИИ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В статье рассматриваются этические вопросы, связанные с искусственным интеллектом, особенно ставшими актуальными в свете появления ChatGPT. Приведены примеры регулирования сферы искусственного интеллекта со стороны Европейского союза, Соединенных штатов Америки и Китайской народной Республики. Остановились на проблеме регулирования сферы искусственного интеллекта и на причинах почему такая проблема в регулировании будет сохраняться: проблема темпа (pacing problem) и дилемма Коллингриджа (Collingridge dilemma).

В качестве возможного решения проблем регулирования искусственного интеллекта указали на опережающее/предвосхищающее управление (anticipatory governance), так называемые «мягкие законы (soft laws)» и «регуляторные песочницы (regulatory sandboxes)». Наконец, отметили, что из фокуса внимания исследователей не должны уходить низкооплачиваемые работники по всему миру, выполняющих повторяющиеся задачи по маркировке и сбору данных для искусственного интеллекта в достаточно тяжелых условиях труда.

Ключевые слова: генеративный искусственный интеллект; ChatGPT; искусственный интеллект; большие данные; этика искусственного интеллекта; регулирование искусственного интеллекта.

Аннотация. Мақалада жасанды интеллектке қатысты этикалық мәселелер қарастырылады, әсіресе ChatGPT пайда болуына байланысты өзекті болды. Еуропалық одақ, Америка Құрама Штаттары және Қытай Халық Республикасы тарапынан жасанды интеллект саласын реттеудің мысалдары келтірілген. Біз жасанды интеллект саласын реттеу мәселесіне тоқталдық және реттеудегі мұндай проблеманың неге сақталатындығына тоқталдық: қарқын мәселесі (pacing problem) және Коллингридж дилеммасы (Collingridge dilemma).

Жасанды интеллектті реттеу мәселелерін ықтимал шешу ретінде «жұмсақ заңдар (жұмсақ заңдар)» және «реттеуші құм жәшіктері (regulatory sandboxes)» деп аталатын алдын ала/алдын ала басқару (anticipatory governance) көрсетілді. Соңында, зерттеушілердің назарынан бүкіл әлем бойынша жасанды интеллект саласы үшін деректерді таңбалау және жинау бойынша қайталанатын

тапсырмаларды орындайтын жалақысы төмен жұмысшылар кетпеу керек екенін атап өтеміз.
Түйінді сөздер: генеративті жасанды интеллект; ChatGPT; жасанды интеллект; үлкен деректер; жасанды интеллект этикасы; жасанды интеллектті реттеу.

Annotation. The article discusses ethical issues related to artificial intelligence, which have become particularly relevant in light of the emergence of ChatGPT. Examples of AI regulation by the European Union, the United States and the People's Republic of China are given. We dwelled on the problem of AI regulation and the reasons why this problem in regulation will persist: the pacing problem and the Collingridge dilemma.

Predictive governance, so-called "soft laws" and "regulatory sandboxes" were pointed out as possible solutions to AI regulation problems. Finally, they noted that the focus of research should not be lost on the low-wage workers around the world who perform repetitive labeling and data collection tasks for artificial intelligence under rather harsh working conditions.
Keywords: generative artificial intelligence; ChatGPT; artificial intelligence; big data; artificial intellect ethics; artificial intelligence regulation.

Актуальность генеративного искусственного интеллекта (далее – ИИ) трудно переоценить благодаря его способности создавать и генерировать новый контент, такой как изображения, тексты и даже музыка. Он имеет множество применений и преимуществ в различных отраслях таких как: генерация креативного контента, персонализация и рекомендательные системы, расширение данных, виртуальные миры и игры, здравоохранение и поиск лекарств, обработка естественного языка, творческие инструменты и помощь в проектировании. Это лишь несколько примеров, иллюстрирующих актуальность генеративного ИИ в различных областях. Его потенциал для автоматизации творческих задач, улучшения процесса принятия решений и повышения качества пользовательского опыта делает его интересной и влиятельной технологией.

Возникновение генеративного искусственного интеллекта оказывает значительное влияние во всем мире, заставляя всех задуматься о его потенциале для повышения эффективности своей работы [1].

Впечатляющие возможности и широкое применение ChatGPT привлекли значительное внимание. Его способность проявлять интеллект и интуицию на поразительном уровне в различных сценариях, включая кодирование, создание контента и ответы на различные вопросы, демонстрирует мощь этого разговорного инструмента ИИ. Используя машинное обучение (Machine learning - ML) и обработку естественного языка (Natural language processing - NLP), ChatGPT уже доказал свою способность генерировать очень ценный и оригинальный контент. Илон Маск, один из основателей OpenAI (покинувший ее в 2018 году), выразил свое удивление в декабрьском твите, заявив, что мастерство ChatGPT одновременно впечатляет и немного нервирует,

свидетельствуя о том, что мы приближаемся к потенциально опасному этапу развития ИИ [2].

Этические проблемы, связанные с искусственным интеллектом.

Согласитесь, в наше время, вряд ли какая-либо автостроительная компания выпустит на дороги общего пользования автомобиль без встроенных систем безопасности. Но по мнению Melissa Heikkilä с MIT Technology review, журналистки специализирующейся на теме искусственного интеллекта, то, что сейчас делают компании-разработчики систем искусственного интеллекта походит на производство спортивных авто без ремней безопасности или не в полную меру функционирующей тормозной системы и с разрешением возможных проблем по мере их поступления [3]. Резонно возникает вопрос, почему же то, что не позволяют себе автостроители, позволяют себе IT-компании?

Такое отношение к мерам предосторожности не могло остаться безнаказанным. В ряде стран начаты расследования в отношении разработчика ставшего шикороизвестным ChatGPT - компании OpenAI: Управлением комиссара по вопросам конфиденциальности Канады (The Office of the Privacy Commissioner of Canada) [4] и Итальянское управление по защите данных (Garante per la protezione dei dati personali) [5]. Другие Европейские страны в свою очередь будут наблюдать за ходом расследования в Италии и по его результатам будут принимать соответствующие меры. Россия, Китай, Сирия, Иран, Северная Корея, Куба пошли дальше и по различным причинам заблокировали работу сервиса [6].

Согласно мнению V. Chiao этические проблемы, связанные с искусственным интеллектом, следует разделить на три группы: проблемы справедливости (fairness), подотчетности (accountability) и прозрачности (transparency) [7; с.127]. Во-первых, если ИИ опирается на необъективную информацию в ее необработанном виде, можем ли мы доверять такому ИИ? Во-вторых, кто должен нести ответственность за неблагоприятные результаты, возникающие в результате использования ИИ? В отличие от людей, споры с алгоритмом могут оказаться столь же плодотворными, как споры с холодильником или тостером. И наконец, насколько важно для нас понимать внутреннюю работу алгоритма и какие последствия вытекают из нашего непонимания логики, используемой ИИ в процессе принятия решений?

Зарубежный опыт регулирования искусственного интеллекта.

В последнее время активно обсуждался вопрос регулирования искусственного интеллекта (ИИ), включая предложения о введении моратория со стороны некоторых ученых и частных лиц. Реакция на эти предложения была различной. Некоторые правительства приняли такие меры, как запрет ChatGPT или установление правил для подобных

ботов ИИ, в то время как другие не предприняли никаких действий до сих пор или могут не предпринять их вообще [8].

Европа занимает лидирующие позиции в области разработки законодательства по регулированию искусственного интеллекта. 11 мая 2023 года ведущие парламентские комитеты Европейского парламента одобрили закон об искусственном интеллекте (AI Act), разработанный два года назад.

Последующий этап предполагает принятие закона на пленарной сессии, предварительно назначенной на 14 июня 2023 года. После того как евродепутаты оформят свою позицию, предложение вступит в заключительную стадию законодательного процесса - переговоры с Советом ЕС и Комиссией, известные как трилогия.

AI Act служит основной законодательной базой для регулирования искусственного интеллекта, учитывая его потенциальную возможность причинения вреда. Закон был совместно одобрен парламентскими комитетами по гражданским свободам и внутреннему рынку, получив поддержку значительного большинства [9].

AI Act разделяет компьютерные программы на основе искусственного интеллекта по трем уровням риска (неприемлемый риск, приложения с высоким уровнем риска, приложения, не запрещенные в явном виде или не отнесенные к категории высокого риска) и исходя из этого отличается и степень регулирования.

Вместе с тем, Адам Терье, автор книги Evasive Entrepreneurs, полагает, что инновации в ИИ, которые появились в США, никогда не появятся в Европе по определению, так как законы этого просто не позволяют. Он полагает, что Европейский подход к регулированию ИИ лишь укрепит власть глобальных IT-гигантов, потому что лишь они могут содержать юридические подразделения, способные привести все в соответствие с нормами AI Act [10].

Вместе с тем, США, которое до настоящего времени считалось своего рода «тихой гаванью» для инноваций в области искусственного интеллекта, с либеральным подходом к регулированию данной сферы предпринимает первые предварительные шаги по установлению правил для инструментов искусственного интеллекта, поскольку ажиотаж вокруг генеративного ИИ и чат-ботов достиг апогея.

11 апреля 2023 года Министерство торговли США объявило о том, что оно официально просит общественность высказать свои замечания по поводу того, как создать меры подотчетности для искусственного интеллекта, и просит помощи в том, как посоветовать американским политикам подходить к этой технологии [11].

Белым домом предложен «Билль о правах ИИ (Blueprint for an AI Bill of Rights)», в котором отраженно пять принципов предотвращения дискриминации и защиты конфиденциальности и безопасности пользователей, а а Национальный институт стандартов и технологий

(National Institute of Standards and Technology) выпустил рамочную программу управления рисками ИИ (AI Risk Management framework).

Однако до сих пор Вашингтон применял добровольный подход к соблюдению требований, в то время как эксперты говорят о необходимости более обязательного подхода к регулированию ИИ [12].

Проект закона под названием «Административные меры для услуг генеративного искусственного интеллекта (Administrative Measures for Generative Artificial Intelligence Services)», опубликованный Администрацией киберпространства Китая (Cyberspace Administration of China), гласит, что национальные агентства по регулированию интернета должны провести оценку безопасности, прежде чем предлагать продукты генеративного ИИ общественности. Цель этого закона - обеспечить ответственное и регулируемое использование технологии генеративного искусственного интеллекта для его здорового развития. Контент, создаваемый ИИ, должен соответствовать основным социалистическим ценностям и не должен содержать материалов, бросающих вызов государственной власти. Кроме того, он не должен содержать террористическую или экстремистскую пропаганду, поощрять этническую ненависть или любой другой контент, способный нарушить экономическую и социальную стабильность [13].

Управление ИИ во всем мире носит фрагментарный характер. Существует также множество инициатив в этой области, включая этические кодексы и принципы ответственного использования ИИ, но они не имеют обязательной силы.

Такая проблема в регулировании будет сохраняться, потому что она коренится в двух вопросах, лежащих в основе управления всеми новыми технологиями, от синтетической биологии до криптовалют, и оба они не поддаются простым решениям. Это проблема темпа (pacing problem) и дилемма Коллингриджа (Collingridge dilemma).

Проблема темпа

Сфера применения, внедрения и распространения технологий развивается быстро, в то время как законы и нормативные акты разрабатываются и принимаются медленнее и обычно регулирование «догоняет» технологии. Применение технологии также является универсальным, в то время как регулирование зависит от конкретной страны.

Кроме того, разработка глобального регулирования требует огромного количества времени и усилий, и они не всегда успешны. Это несоответствие называется проблемой темпа.

Что еще хуже, проблема темпа усиливается комбинаторными инновациями: технологические и развивающие возможности, которые быстро и симбиотически наращиваются друг на друга для ускорения инноваций.

дилемма Коллингриджа

Дэвид Коллингридж представил концепцию, известную сегодня как дилемма Коллингриджа. Дилемма заключается в том, что регулирование технологии на начальных этапах ее внедрения, когда ее потенциальные опасности еще не очевидны, является легкой задачей, но становится сложнее к тому времени, когда эти опасности выявлены.

«Раннее регулирование, скорее всего, будет слишком ограничительным для дальнейшего развития и внедрения, в то время как регулирование на более зрелой стадии может быть ограничено в своей эффективности и способности предотвращать несчастные случаи» [8].

Возможные пути решения к регулированию ИИ.

Некоторые способы решения проблемы темпа и дилеммы Коллингриджа включают в себя опережающее/предвосхищающее управление (anticipatory governance), так называемые «мягкие законы (soft laws)» и «регуляторные песочницы (regulatory sandboxes)».

Предвосхищающее управление — это концепция и практика, использующие предвидение грядущих событий для руководства политикой и практикой в настоящем. Мы можем предвидеть лучше, если мы регулярно и содержательно взаимодействуем с заинтересованными сторонами и имеем гибкое управление.

«Мягкие законы» включают добровольные руководства, стандарты, установленные промышленностью, а также принципы и механизмы, разработанные на основе консенсуса, часто при косвенной роли регулирующих органов. Мягкие законы могут не иметь юридической силы, но они проводят четкую грань между тем, что можно и что нельзя делать, и могут дополнять нормативные акты.

«Регуляторная песочница» – это инструмент, который позволяет новаторам экспериментировать с новыми продуктами или услугами под надзором регулятора. В процессе регулятор также понимает технологию, контекст, в котором она будет применяться, и то, какие возможности выбора она предоставит заинтересованным сторонам.

Принятие этих стратегий поможет решить проблему темпов и дилемму Коллингриджа, а также даст регулирующим органам определенный контроль и предсказуемость в отношении ИИ. Но будут ли они идеальным решением, на данный момент предсказать сложно [8].

И в заключении хотелось бы отметить, что фокусируясь на виртуальных проблемах, от внимания исследователей и политиков выпадают проблемы реального мира.

Технологические компании зависят от работников, таких как маркировщики данных, водители доставки и модераторы контента. По данным исследователей этого вопроса, технологический прогресс в сфере ИИ подпитывается миллионами низкооплачиваемых работников по всему миру, выполняющих повторяющиеся задачи в тяжелых условиях труда. И в отличие от «исследователей ИИ», получающих

шестизначные зарплаты в корпорациях Кремниевой долины, эти работники часто нанимаются из бедных слоев населения и получают всего $1,46/час после уплаты налогов. Однако, несмотря на это, эксплуатация труда не занимает центральное место в дискуссии вокруг этической разработки и внедрения систем ИИ. В своей статье Adrienne Williams и др. приводят примеры трудовой эксплуатации, лежащей в основе так называемых систем ИИ, и они поднимают вопрос о том, что поддержка усилий по организации транснациональных рабочих должна быть приоритетом в дискуссиях, касающихся этики ИИ.

В то время как исследователи этичного ИИ, ИИ для социального блага или ИИ, ориентированного на человека, в основном сосредоточены на «очистке» данных и обеспечении прозрачности и справедливости моделей, полагаем, что прекращение эксплуатации труда в индустрии ИИ не должно уходить от внимания исследователей и политиков [14].

Список использованных источников:

1. The Hype And The Reality Of Using Generative AI In Sales. // The Forbes: [Electronic resource] – Access mode: https://www.forbes.com/sites/forrester/2023/04/20/the-hype-and-the-reality-of-using-generative-ai-in-sales/?sh=40d9b15b1699 (Access date: 22.04.2023).
2. Is ChatGPT Worthy of All the Hype?. // International banker: [Electronic resource] – Access mode: https://internationalbanker.com/technology/is-chatgpt-worthy-of-all-the-hype/ (Access date: 19.04.2023).
3. Heikkilä A Cambridge Analytica-style scandal for AI is coming / Heikkilä. // MIT Technology review: [Electronic resource] – Access mode: https://www.technologyreview.com/2023/04/25/1072177/a-cambridge-analytica-style-scandal-for-ai-is-coming/ (Access date: 01.05.2023).
4. Announcement: OPC launches investigation into ChatGPT. // Office of the Privacy Commissioner of Canada: [Electronic resource] – Access mode: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/ (Access date: 30.04.2023).
5. Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori. — Текст : электронный // Garante per la protezione dei dati personali: [Electronic resource] – Access mode: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english_ (Access date: 01.05.2023).
6. Martindale, J. These are the countries where ChatGPT is currently banned / J. Martindale. [Electronic resource] – Access mode: https://www.digitaltrends.com/computing/these-countries-chatgpt-banned/ (Access date: 03.05.2023).
7. Chiao V. Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice //International Journal of Law in Context. – 2019. – Т. 15. – №. 2. – С. 126-139.
8. Srinivas Two reasons AI is hard to regulate: the pacing problem and the Collingridge dilemma / Srinivas. [Electronic resource] – Access mode: https://www.thehindu.com/sci-tech/science/ai-regulation-pacing-problem-collingridge-dilemma/article66802967.ece (Access date: 04.05.2023).

9. Bertuzzi AI Act moves ahead in EU Parliament with key committee vote. / Bertuzzi. // Euractiv: [Electronic resource] – Access mode: https://www.euractiv.com/section/artificial-intelligence/news/ai-act-moves-ahead-in-eu-parliament-with-key-committee-vote/ (Access date: 16.05.2023).

10. Thierer Why the Future of AI Will Not Be Invented in Europe. Technology Liberation Front. / Thierer. //: [Electronic resource] – Access mode: https://techliberation.com/2022/08/01/why-the-future-of-ai-will-not-be-invented-in-europe/ (Access date: 18.04.2023).

11. Bhuiyan 'We have to move fast': US looks to establish rules for artificial intelligence. / Bhuiyan. // The Guardian: [Electronic resource] – Access mode: https://www.theguardian.com/technology/2023/apr/11/us-commerce-department-artificial-intelligence-rules (Access date: 01.05.2023).

12. Iyengar AI Regulation Fever Sweeps EU, US, and China. / Iyengar. // Foreign Policy: [Electronic resource] – Access mode: https://foreignpolicy.com/2023/05/05/eu-ai-act-us-china-regulation-artificial-intelligence-chatgpt/ (Access date: 11.05.2023).

13. Iyengar China to require 'security assessment' for new AI products: draft law / Iyengar. // France 24: [Electronic resource] – Access mode: https://www.france24.com/en/live-news/20230411-china-to-require-security-assessment-for-new-ai-products-draft-law (Access date: 20.04.2023).

14. Williams The Exploited Labor Behind Artificial Intelligence. / Williams. // NOEMA. [Electronic resource] – Access mode: https://www.noemamag.com/the-exploited-labor-behind-artificial-intelligence/ (Access date: 02.05.2023).

УДК 34.343.2/.7

Серімбетов Нұрбол Нұрланұлы
Магистрант Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан,
г. Астана, Республика Казахстан

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЛАЧНЫХ СИСТЕМ

Аннотация. В статье проведен анализ развития и становления правовой базы в части использования и защиты персональных данных, хранящихся в облачных системах, с учетом изменения реалий и развития технологий.

Отмечено, что многие страны внедряют в свои законодательства положения, касающиеся использования облачных технологий в различных сферах, в том числе и в правоохранительной деятельности.

Установлено, что в Уголовно-процессуальном кодексе РК не содержится прямого упоминания об облачных технологиях, однако в соответствии с Конституцией РК и другими законодательными актами государства, соблюдение конфиденциальности персональных данных является обязательным. Таким образом, доступ к информации, содержащейся в облачных системах, возможен только при наличии санкции суда и с учетом требований законодательства о персональных данных. Несмотря на то, что в Казахстане существует закон «О персональных данных и их защите», который регулирует общественные отношения в сфере персональных данных, данный закон не содержит нормативных актов, регулирующих облачные хранилища как таковые. Это может создавать определенные проблемы для граждан, которые хранят свои данные в облачных системах. Для решения этой проблемы необходимо внести поправки в законодательство, которые бы учитывали современные технологии и требования пользователей.

Ключевые слова: облачные хранилища; защита персональных данных; использование облачных технологий в расследовании преступлений

Аннотация. Мақалада шындықтың өзгеруі мен технологияның дамуын ескере отырып, бұлтты жүйелерде сақталған дербес деректерді пайдалану және қорғау бөлігінде құқықтық базаның дамуы мен қалыптасуына талдау жасалды.

Көптеген елдер өз заңнамаларына әртүрлі салаларда, соның ішінде құқық қорғау қызметінде бұлтты технологияларды қолдануға қатысты ережелерді енгізіп жатқаны атап өтілді.

ҚР Қылмыстық-процестік кодексінде бұлтты технологиялар туралы тікелей айтылмайтыны анықталды, алайда ҚР Конституциясына және мемлекеттің басқа да заңнамалық актілеріне сәйкес дербес деректердің құпиялылығын сақтау міндетті болып табылады. Осылайша, бұлтты жүйелердегі ақпаратқа қол жеткізу тек соттың санкциясы болған кезде және жеке деректер туралы заңнаманың талаптарын ескере отырып мүмкін болады. Қазақстанда дербес деректер саласындағы қоғамдық қатынастарды реттейтін "Дербес деректер және оларды қорғау туралы" заң бар екеніне қарамастан, бұл заңда бұлтты сақтауды реттейтін нормативтік актілер жоқ. Бұл өз деректерін бұлтты жүйелерде сақтайтын азаматтар үшін белгілі бір проблемалар тудыруы мүмкін. Бұл мәселені шешу үшін заманауи технологиялар мен пайдаланушылардың талаптарын ескеретін заңнамаға түзетулер енгізу қажет.

Түйінді сөздер: бұлттық қойма; жеке деректерді қорғау; қылмысты тергеуде

бұлттық технологияны қолдану

Annotation. The article analyzes the development and formation of the legal framework regarding the use and protection of personal data stored in cloud systems, taking into account changing realities and technology development.

It is noted that many countries are introducing into their legislation provisions concerning the use of cloud technologies in various fields, including in law enforcement.

It is established that the CPC of the Republic of Kazakhstan does not contain a direct mention of cloud technologies, however, in accordance with the Constitution of the Republic of Kazakhstan and other legislative acts of the state, the confidentiality of personal data is mandatory. Thus, access to information contained in cloud systems is possible only if there is a court order and taking into account the requirements of the legislation on personal data. Despite the fact that in Kazakhstan there is a law "On personal data and their protection", which regulates public relations in the field of personal data, this law does not contain regulations regulating cloud storage as such. This can create certain problems for citizens who store their data in cloud systems. To solve this problem, it is necessary to amend legislation that would take into account modern technologies and user requirements.

Keywords: cloud storage; personal data protection; use of cloud technologies in crime investigation

С развитием технологий и переходом многих компаний на использование облачных технологий, информационные системы стали более сложными, а также стали содержать огромное количество ценной информации. Облачные системы позволяют пользователям хранить данные и приложения удаленно, а также совместно работать с ними через Интернет. Таким образом, облачные системы стали ключевым фактором в хранении и обработке данных, особенно для компаний.

Цель статьи заключается в проведении анализа развития и становления правовой базы в части использования и защиты персональных данных, хранящихся в облачных системах.

Научные исследования, посвященные облачным технологиям, включают различные подходы к их исследованию и толкованию.

Ученые толкуют облачные хранилища по-разному в зависимости от их научного направления и задач, которые они решают.

Российский ученый Бутнев В., отмечает: «Облачные хранилища - это способ организации хранения и обработки большого объема данных с использованием удаленных серверов, доступных через Интернет» [1].

«Облачные хранилища - это новый этап в развитии технологий, которые позволяют организовывать удаленный доступ к данным и ресурсам с использованием облачных платформ» - об этом нам толкует М.В. Строганов [2].

Большинство ученых считают, что облачные хранилища - это удаленные серверы, которые позволяют пользователям хранить, управлять и обрабатывать свои данные через интернет и рассматривают облачные хранилища как эффективный способ хранения и обработки данных, который обладает рядом преимуществ, включая

гибкость, масштабируемость, доступность и снижение затрат на оборудование и поддержку. Они считают, что облачные хранилища могут стать ключевым элементом цифровой трансформации в различных секторах экономики, включая судебную систему.

Однако, другие ученые высказывают опасения относительно безопасности и конфиденциальности данных в облачных хранилищах, особенно в свете возможных угроз со стороны киберпреступников и правительственных органов. Они также обращают внимание на риск потери контроля над данными, когда они хранятся в удаленных серверах, а также на проблемы, связанные с юрисдикцией и международными правовыми нормами в отношении доступа к данным, которые хранятся в других странах.

В этой связи многие страны внедряют в свои законодательства положения, касающиеся использования облачных технологий в различных сферах, в том числе и в правоохранительной деятельности. Некоторые примеры кодексов, в которых содержатся положения про облачные технологии:

Федеральный закон США Electronic Communications Privacy Act (далее ECPA) принят в 1986 году и регулирует сбор, использование и раскрытие электронной коммуникации в США. ECPA устанавливает правила для правительственных и частных лиц относительно доступа к электронной коммуникации, такой как электронная почта, текстовые сообщения, файлы, хранящиеся в облачных хранилищах и т.д. [3] По ECPA, правительственным организациям требуется получать ордер от судьи для доступа к содержанию электронной коммуникации, а также для доступа к информации, хранящейся в облачных системах.

В соответствии с разделом 18 Свода законов США, § 2703, государственные органы могут запрашивать доступ к электронным записям и сообщениям клиентов у поставщиков услуг связи в определенных обстоятельствах. Такие обстоятельства могут включать, например, случаи, когда такой доступ требуется для расследования преступлений или для обеспечения национальной безопасности.

Однако, в соответствии с ECPA, поставщики услуг связи должны соблюдать определенные процедуры при предоставлении доступа к записям и сообщениям клиентов государственным органам. В частности, они должны получить судебное распоряжение или предъявить другие юридически обоснованные основания для получения такого доступа.

Кроме того, ECPA предоставляет клиентам определенные права в отношении конфиденциальности и частной жизни. Например, поставщики услуг связи должны уведомлять клиентов о запросах на их записи и сообщения, если это юридически допустимо. Клиенты также имеют право на защиту от незаконного доступа к их электронным записям и сообщениям.

Облачные вычисления значительно улучшают возможности

сетевого хранения, предоставляя доступ по запросу к общему пулу настраиваемых вычислительных ресурсов (например, к сетям, серверам, хранилищам, приложениям, и услуги), которые могут быть быстро предоставлены и выпущены с минимальными усилиями по управлению или взаимодействием с поставщиком услуг.

Независимо от того, применяются ли они к внутренним бизнес-показателям или системе электронной почты, облачные вычисления повышают эффективность и снижают затраты на информационные технологии.

Но облачные вычисления предполагают рассредоточение данных по серверам, расположенным в любой точке мира. То, как облако выходит за национальные границы, создает потенциальную опасность, поскольку данные перемещаются или разрешается доступ к данным из стран с ограничительными законами о конфиденциальности и защите данных. Если, например, компания, использующая облако для хранения электронной информации, оказывается втянутой в расследование или судебный процесс, она должна учитывать соответствующие законы перед сбором, проверкой и созданием соответствующих электронных данных.

Защита облачных данных — это набор мер по хранению данных и безопасности, предназначенных для защиты данных, находящихся в облачной среде, а также перемещаемых в нее и из нее. Когда дело доходит до рассматриваемых данных, сохраненные данные называются «данными в состоянии покоя», а движущиеся данные — «данными в движении» [4].

Облачные данные обычно защищаются с помощью таких методов, как резервное копирование, облачное хранилище и аварийное восстановление — все они предназначены для обеспечения того, чтобы данные оставались во владении организации в случае утечки вредоносного ПО, потери данных или другого события, которое может использовать уязвимость облачных данных.

Большинство законов о конфиденциальности и защите данных принимаются для защиты личной информации граждан каждой страны [5]. Эти законы обычно регулируют способность юридических и физических лиц «обрабатывать» (т.е. собирать, сохранять, организовывать, хранить, использовать и т. д.) данные других лиц, и они применяются, когда информация хранится, собирается, обрабатывается или передается из страны. Учитывая все более широкое использование мобильных устройств в деловых целях, например, гражданин Мексики, работающий в Канаде, чьи сообщения хранятся у поставщика услуг облачных вычислений, расположенного в Бразилии, вероятно, приведет к срабатыванию определенных положений в рамках законодательных схем всех трех стран.

Основное внимание в большинстве законов о конфиденциальности

данных уделяется согласию: для обработки личной информации работника работодатель (т. е. «пользователь данных») обычно должен сначала получить согласие работника (т. е. «владельца данных») на это. Например, в соответствии с испанским законодательством пользователи данных должны получить письменное согласие от владельцев данных, и это согласие может быть отозвано в любое время.

Некоторые законы о конфиденциальности данных включают исключение из получения согласия при сборе или обработке персональных данных в связи с судебным разбирательством или с целью выполнения юридических обязательств.

Например, закон Аргентины о конфиденциальности данных включает такое исключение, но, тем не менее, гласит, что любая трансграничная передача персональных данных за пределы Аргентины может осуществляться только в страны, обеспечивающие аналогичную защиту данных (т. е. не в Соединенные Штаты), за исключением случаев, когда передача осуществляется в соответствии с: (1) явным согласием, (2) подписанным соглашением о передаче данных, подготовленным под руководством регулирующего органа, (3) международным судебным сотрудничеством или (4) другими ограниченными исключениями [6].

Кроме того, необходимо понимать требования к безопасности и отчетности для каждого соответствующего режима конфиденциальности данных.

В Мексике Федеральный закон 2010 года о защите персональных данных, находящихся в распоряжении частных лиц, требует соблюдения стандартных для отрасли мер физической, технической и административной безопасности, предназначенных для защиты персональных данных от несанкционированного повреждения, изменения, потери или использования [7]. Более того, в случае утечки персональных данных пользователи данных должны незамедлительно уведомить всех и каждого владельца данных, чьи персональные данные могли быть затронуты. Это общее требование, поэтому компании, использующие службы облачных вычислений, должны иметь коммуникационные процессы, способные быстро и эффективно уведомлять сотрудников или других владельцев данных о любом потенциальном нарушении безопасности.

Закон Аргентины о защите данных требует, чтобы все пользователи данных регистрировали общедоступные и частные базы данных в своем агентстве по защите данных. Однако, поскольку закон Аргентины был принят в 2000 году, он, по понятным причинам, не полностью предусматривает текущее использование облачных или интернет-сетей, физически расположенных за пределами Аргентины, но достигающих страны для электронных личных данных. По этой причине неясно, насколько далеко простираются требования Аргентины о

регистрации. Хотя кажется очевидным, что компания, устанавливающая сервер в Аргентине для использования сотрудниками, работающими в стране, попадает под это требование, нет никаких указаний относительно того, как это требование может применяться к облачной системе, которая распространяется на страну. Если закон работает аналогично закону о защите данных в Испании, пользователь данных, зарегистрированный в Аргентине, должен зарегистрировать свою базу данных и указать своего поставщика облачных услуг (т. е. обработчика данных). В свою очередь, этот поставщик попадает под действие закона, даже если он (и его субподрядчики) фактически находится за пределами Аргентины [7].

В некоторых странах, например в Уругвае, прямо разрешена трансграничная передача персональных данных между группой компаний или внутри нее без какого-либо дополнительного разрешения в ситуациях, когда материнская, дочерняя, аффилированная компания или филиал, получающие персональные данные, должным образом приняли кодекс поведения и зарегистрировали в соответствующем органе по защите данных. Опять же, если корпорация работает в нескольких странах, следует изучить такие требования, прежде чем размещать электронные данные в облаке [5].

Наконец, компании следует изучить механизмы правоприменения и возможные санкции, связанные с любым нарушением применимого режима конфиденциальности данных.

Мексика, например, создала федеральное агентство Instituto Federal de Acceso a la Información (или «IFAI») для надзора за режимом защиты данных 2010 года. IFAI, обладающая оперативной, бюджетной автономией и самостоятельностью в принятии решений, отвечает, среди прочего, за упреждающий мониторинг и обеспечение соблюдения правил защиты данных, реагирование на жалобы владельцев данных и наложение санкций за несоблюдение. IFAI применила свои правоприменительные полномочия в частном секторе, наложив несколько серьезных санкций после вступления в силу мексиканского закона [5].

27 апреля 2016 года в ЕС был принят Общий Регламент защиты персональных данных (General Data Protection Regulation). GDPR-compliance – это выстраивание бизнес-процессов компании в соответствии с правилами Регламента. При внедрении GDPR компании зачастую используют план действий, который содержится в стандарте ISO 27701 (Управление информационной безопасностью) [8]. Задуматься о соответствии GDPR стоит каждой компании, деятельность которой так или иначе связана с Евросоюзом. При этом, чтобы находиться под действием Регламента, даже не обязательно иметь офисы в странах ЕС. GDPR не действует на компании, а применяется к отдельным процессам («обработкам») с персональными данными. Для

одних компаний под GDPR окажутся все обработки, а для других – лишь некоторые процессы.

GDPR пришел на смену директивы от 1995 года [8]. За более чем 20 лет бизнес-процессы изменились драматически. Появились такие компании как Facebook, Uber, Booking, Yandex и многие другие, которым мы всецело доверяем личную информацию, переписку, фотографии, предпочтения. Объем данных, которые хранятся в «облаке», растет год от года, так же, как и их критичность. К сожалению, киберпреступники активно используют уязвимости онлайн-систем и сообщения об инцидентах с утечкой данных, кражи номеров банковских карт появляются в СМИ все чаще.

Затрагивает ли GDPR Казахстан? Да. В официальном определении из закона о применимости GDPR есть пункт с пояснениями. Во-первых, это может быть компания или организация с офисом в Европейском союзе, которая обрабатывает персональные данные в рамках своей операционной деятельности, несмотря на то, где данные обрабатываются. Во-вторых, компания не из ЕС, предлагающая товары/услуги (платно или бесплатно) или осуществляющая мониторинг поведения физических лиц из ЕС. Таким образом, если предприятие из Казахстана целенаправленно работает на рынок ЕС (имеет языковые версии сайтов, буклетов стран ЕС, принимает европейскую валюту), то оно должно соответствовать нормам GDPR. Обратите внимание, что речь не про граждан ЕС, а о физических лицах ЕС. Если я, как гражданин Казахстана, поехал в командировку в Германию и совершаю покупки или пользуюсь сервисами из России или Казахстана (например, Qiwi-кошелек), то такой сервис для работы со мной должен соответствовать GDPR. Кого в Казахстане может затронуть европейское регулирование? Например, банки, мобильных операторов, авиаперевозчиков и всех тех, кто работает с пользователями (не обязательно гражданами) из ЕС. Новый регламент на 80% — это ИТ-инфраструктура компании. 20% - разработка методик и других документов, которыми компания будет руководствоваться в различных ситуациях. Готовы ли к этому казахстанские компании? Вряд ли.

Уголовно-процессуальный кодекс Республики Казахстан (далее - УПК РК) предусматривает необходимость сбора доказательств и допроса свидетелей в рамках досудебного расследования уголовных дел. Современные технологии, такие как облачные системы, могут содержать важную информацию, необходимую для установления фактов преступлений. – 1 УПК РК [9].

В УПК РК не содержится прямого упоминания об облачных технологиях, однако в соответствии с Конституцией РК и другими законодательными актами государства, соблюдение конфиденциальности персональных данных является обязательным. Таким образом, доступ к информации, содержащейся в облачных

системах, возможен только при наличии санкции суда и с учетом требований законодательства о персональных данных.

В Российской Федерации законом, регулирующим персональные данные, является Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [10]. Данный закон содержит статьи, в которых упоминаются облачные системы хранения данных.

Например, статья 6 ФЗ от 27 июля 2006 года № 152-ФЗ «О персональных данных» устанавливает принципы обработки персональных данных, включая обоснованность, справедливость и законность, а также требования к защите персональных данных от несанкционированного доступа. При использовании облачных систем для обработки персональных данных, организации должны обеспечивать соответствующую защиту персональных данных.

Статья 18 ФЗ от 27 июля 2006 года № 152-ФЗ «О персональных данных» регулирует передачу персональных данных третьим лицам, требуя согласия субъекта персональных данных, кроме случаев, когда передача данных является необходимой для выполнения закона или договора. Если организации используют облачные системы хранения данных для передачи персональных данных, они также должны соблюдать эти правила.

Статья 19 ФЗ от 27 июля 2006 года № 152-ФЗ «О персональных данных» устанавливает правила доступа субъектов персональных данных к своим данным. Организации, использующие облачные системы хранения данных, также должны обеспечивать доступ субъектов персональных данных к своим данным.

Таким образом, законодательство Российской Федерации устанавливает требования к обработке, передаче и доступу к персональным данным в облачных системах хранения данных, обеспечивая защиту персональных данных и права субъектов персональных данных.

Несмотря на то, что в Казахстане существует закон «О персональных данных и их защите» [11], который регулирует общественные отношения в сфере персональных данных, данный закон не содержит нормативных актов, регулирующих облачные хранилища как таковые. Это может создавать определенные проблемы для граждан, которые хранят свои данные в облачных системах.

Для решения этой проблемы необходимо внести поправки в законодательство, которые бы учитывали современные технологии и требования пользователей. Примером может служить опыт зарубежных стран, где существуют законы, регулирующие облачные хранилища и обеспечивающие защиту персональных данных в таких системах.

Заключение. Во многих странах, в том числе, и в Казахстане, в законодательстве отсутствует четкое регулирование «облаков». Законодательство Казахстана не содержит термина «облачные

технологии». Однако, концепция «облака» частично предусмотрена законодательством Казахстана (платформа e-gov).

В целом, использование облачных технологий может привести к:

• трансграничной передаче данных

• передаче персональных данных

• использованию «облачных» решений различными пользователями (государственными, частными).

Принимая во внимание, что пользователь «облака» может передавать различные виды данных за пределы Казахстана, следует учитывать положения местного законодательства.

Использование «облачных» технологий в Казахстане следует рассматривать со следующих точек зрения:

• Неприкосновенность персональных данных;

• Частные и государственные конфиденциальные данные;

• Регулирование доменов;

• Отраслевое регулирование: организации финансового сектора, телекоммуникации и государственный сектор.

Согласно Закону о персональных данных, хранение персональных данных осуществляется собственником и (или) оператором или третьей стороной, осуществляющей действия от имени собственника или оператора, в базе данных («База данных»), расположенной на территории Республики Казахстан. В то же время трансграничная передача персональных данных разрешена, если страна, куда передаются такие персональные данные, предоставляет защиту таких данных. Закон о персональных данных не устанавливает ограничений на использование «облака», расположенного за пределами Казахстана для передачи и хранения данных.

Для сравнения, аналогичный закон в Российской Федерации содержит требование, чтобы «сбор, запись, систематизация, аккумулирование, хранение, исправление (обновления, изменения) и выборка» таких данных осуществлялась в базах данных, расположенных в Российской Федерации. Между тем, закон Республики Казахстан требует, чтобы только хранение персональных данных осуществлялось в базах данных, находящихся на территории Республики Казахстан. Более того, законодательство Российской Федерации требует от «операторов» обеспечить соблюдение указанного требования, тогда как закон Республики Казахстан просто устанавливает, что хранение персональных данных осуществляется в базах данных, находящихся в Республике Казахстан. В определённой степени, существует различие в уровне императивности инструкций/требований, предусмотренных двумя законами/юрисдикциями.

В Законе Республики Казахстан от 24 ноября 2015 года «Об информатизации» [12] *(далее - Закон)* используется термин

«электронные информационные ресурсы», что в целом подразумевает «данные». В частности, термин «данные» определен как информация, представленная в электронно-цифровой форме и содержащаяся на электронном носителе, в интернет ресурсах и(или) в информационной системе.

Согласно Закону, данные подразделяются на следующие типы:

В зависимости от формы собственности:

• государственные;

• негосударственные.

В зависимости от уровня доступности:

• публичные;

• с ограниченным доступом.

Закон предусматривает, что собственник данных вправе использовать и распространять их, при условии соблюдения ограничений, предусмотренных законодательством Казахстана. Существуют ограничения на передачу за границу данных с ограниченным доступом. Таким образом, прочая информация (т. е. публичная) может передаваться без ограничений.

Закон не предусматривает никаких ограничений и запретов касательно использования «облачных» сервисов и технологий ни в государственном, ни в частном секторе. Закон не предусматривает концепции и/или термина «облачных» технологий, а также, не предусматривает сценариев, как различные типы данных должны собираться, использоваться, храниться и передаваться в контексте использования облачных сервисов и технологий.

Правила регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета [13] разработаны в соответствии с подпунктом 16) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года «Об информатизации» и определяют порядок регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета. Требованием к серверному оборудованию регистранта является его физическое нахождение на территории Республики Казахстан (далее – «Требование»). В регистрации .KZ Домена должно быть отказано если, среди прочего, серверное оборудование, на котором будет использоваться интернет-ресурс с заявляемым доменным именем, находится за пределами Республики Казахстан. Регистрация .KZ Домена может быть приостановлена, по такому же основанию, с дальнейшей отменой регистрации .KZ Домена. Согласно официальной позиции уполномоченного органа, Требование к .KZ Домену относится к серверному оборудованию, на котором осуществляется хостинг .KZ Домена и не распространяется на серверное оборудование сервисов связанных с KZ. Доменом. Таким образом, за исключением «облачных» сервисов предусматривающих хостинг .KZ Домена, Требование не

распространяется на остальные «облачные» сервисы (продукты).

Законодательство Казахстана относительно финансовых организаций (банки, страховые компании и прочее) и телекоммуникационных компаний не содержит каких-либо прямых ограничений для таких финансовых организаций и телекоммуникационных компаний по передаче данных и использованию «облаков». К защите конфиденциальной информации и персональных данных в сфере банковских и телекоммуникационных услуг применяются общие положения по регулированию, хотя не предусмотрены ограничения на использование «облаков». Не предусмотрены ограничения на передачу данных в других отраслях.

Список использованных источников:

1. Общие положения облачных технологий как концептуальной основы комплексной защиты информационных систем. [Электронный ресурс] – Режим доступа: https://www.researchgate.net/publication/334875158_Obshie_polozheniya_oblacloud_tekhnologiy_kak_kontseptualnoy_osnovy_kompleksnoy_zashchity_informatsionnykh_sistem (дата обращения 20.03.2023 г.)
2. Облачные технологии как ресурсный потенциал развития информационной бизнес-структуры. [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/oblachnye-tehnologii-kak-ressursnyy-potentsial-razvitiya-informatsionnoy-biznes-struktury (дата обращения 20.03.2023 г.)
3. Закон о конфиденциальности электронных коммуникаций 1986 г. (ECPA). [Электронный ресурс] – Режим доступа: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (дата обращения 20.03.2023 г.)
4. Что такое облачная защита данных? [Электронный ресурс] – Режим доступа: https://www.zscaler.com/resources/security-terms-glossary/what-is-cloud-data-protection (дата обращения 20.03.2023 г.)
5. Понимание пересечения между законами о конфиденциальности данных и облачными вычислениями. [Электронный ресурс] – Режим доступа: https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing (дата обращения 20.03.2023 г.)
6. Закон о защите персональных данных (PDPA) Аргентины. [Электронный ресурс] – Режим доступа: https://learn.microsoft.com/ru-ru/compliance/regulatory/offering-pdpa-argentina (дата обращения 20.03.2023 г.)
7. Коровяковский Д.Г. Российский и зарубежный опыт в области защиты персональных данных // Национальные интересы: приоритеты и безопасность. 2009. №5. [Электронный ресурс] – Режим доступа: https://cyberleninka.ru/article/n/rossiyskiy-i-zarubezhnyy-opyt-v-oblasti-zaschity-personalnyh-dannyh (дата обращения: 23.03.2023 г.).
8. Что такое GDPR. [Электронный ресурс] – Режим доступа: https://data-privacy-office.com/what-is-gdpr/ (дата обращения 20.03.2023 г.)
9. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 26.03.2023 г.). [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=31575852&show_di=1 (дата обращения 20.03.2023 г.)
10. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция). [Электронный ресурс] – Режим доступа:

http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 20.03.2023 г.)

11. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 03.03.2023 г.). [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=31396226 (дата обращения 20.03.2023 г.)

12. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 01.04.2023 г.). [Электронный ресурс] – Режим доступа: https://online.zakon.kz/m/amp/download/33885902 (дата обращения 03.04.2023 г.)

13. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 13 марта 2018 года № 38/НҚ. Об утверждении Правил регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета (с изменениями и дополнениями по состоянию на 14.10.2022 г.). [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=35205534&doc_id2=32729960#pos=3;-98.33332824707031&pos2=68;-60.33332824707031 (дата обращения 03.04.2023 г.)

УДК 004.8

Тюгинбаев Думан Дулатович
Старший прокурор Отдела по развитию и сопровождению
информационно-коммуникационных систем
Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан,
г. Астана, Республика Казахстан

К ВОПРОСУ О ФУНКЦИОНИРОВАНИИ ЯЗЫКОВЫХ МОДЕЛЕЙ: КАК РАБОТАЕТ CHATGPT

Аннотация. Языковые модели LLM (Large Language Model) в последние годы стали свидетелями значительного прогресса, совершив революцию в области обработки естественного языка. Эти модели, использующие передовые методы глубокого обучения и огромные объемы обучающих данных, продемонстрировали замечательные возможности в понимании и создании человекоподобного текста.

В статье мы исследуем достижения и инновации, которые сформировали языковые модели LLM, позволив им понимать и генерировать текст с растущей беглостью, контекстуальностью и точностью. Мы углубляемся в ключевые техники и методологии, используемые при обучении этих моделей, такие как обучение без контроля, механизмы самовнимания и архитектуры трансформаторов.

А также более подробно остановимся на принципах работы ChatGPT как яркого образчика LLM.

Ключевые слова: генеративный искусственный интеллект; искусственный интеллект; большие данные; языковые модели; ChatGPT.

Аннотация. LLM (Large Language Model) тілдік модельдері соңғы жылдары табиғи тілді өңдеуде төңкеріс жасап, айтарлықтай прогреске куә болды. Терең оқытудың озық әдістерін және көптеген оқу деректерін қолданатын бұл модельдер адам тәрізді мәтінді түсіну мен құрудың керемет мүмкіндіктерін көрсетті.

Мақалада біз LLM тілдік модельдерін қалыптастырған жетістіктер мен инновацияларды зерттейміз, оларға мәтінді еркін, контекстік және дәлдікпен түсінуге және құруға мүмкіндік береміз. Осы модельдерді оқытуда қолданылатын негізгі әдістер мен әдістемелерге тереңірек үңілеміз, мысалы, бақылаусыз оқыту, өзін-өзі ойлау механизмдері және трансформатор архитектурасы.

Сондай-ақ, CHATGPT-дің жарқын LLM үлгісі ретінде жұмыс істеу принциптеріне толығырақ тоқталайық.

Түйінді сөздер: генеративті жасанды интеллект; жасанды интеллект; үлкен деректер; тілдік модельдер; ChatGPT.

Annotation. LLM (Large Language Model) language models have witnessed significant progress in recent years, revolutionizing the field of natural language processing. These models, using advanced deep learning techniques and huge amounts of training data, have demonstrated remarkable capabilities in understanding and creating human-like text.

In this article, we explore the achievements and innovations that have shaped LLM language models, enabling them to understand and generate text with increasing fluency, contextuality and accuracy. We delve into the key techniques and methodologies used in

the training of these models, such as unsupervised learning, self-awareness mechanisms and transformer architectures.

And also let's take a closer look at the principles of ChatGPT as a bright example of LLM.

Keywords: generative artificial intelligence; artificial intelligence; big data; language models; ChatGPT.

Языковые модели LLM (Large Language Model) в последние годы стали свидетелями значительного прогресса, совершив революцию в области обработки естественного языка. Эти модели, использующие передовые методы глубокого обучения и огромные объемы обучающих данных, продемонстрировали замечательные возможности в понимании и создании человекоподобного текста [1].

В этой статье мы исследуем достижения и инновации, которые сформировали языковые модели LLM, позволив им понимать и генерировать текст с растущей беглостью, контекстуальностью и точностью. Мы углубляемся в ключевые техники и методологии, используемые при обучении этих моделей, такие как обучение без контроля, механизмы самовнимания и архитектуры трансформаторов.

Языковые модели LLM используют масштабные наборы данных из различных источников, что позволяет им улавливать все тонкости человеческого языка. Предварительное обучение этих моделей на массивных корпорациях с последующей тонкой настройкой на конкретных задачах доказало свою эффективность в переносе знаний между доменами и достижении передовых результатов в различных задачах обработки естественного языка, включая классификацию текстов, машинный перевод, анализ настроения, ответы на вопросы и резюмирование текстов [2].

Внедрение новых методов, таких как моделирование языка по маске, позволяет моделям LLM обрабатывать неполный или неоднозначный текст, предсказывая пропущенные слова в заданном контексте. Этот метод способствует более глубокому пониманию структуры и смысла языка, улучшая общее понимание языка и контекстное мышление.

Кроме того, недавние исследования были направлены на решение этических проблем и предубеждений, связанных с языковыми моделями LLM. Были предприняты усилия, чтобы смягчить предубеждения, присутствующие в обучающих данных, обеспечить справедливость и инклюзивность, а также способствовать ответственному использованию этих моделей в деликатных приложениях.

Кроме того, языковые модели LLM продемонстрировали перспективность в многоязычных условиях, где они демонстрируют превосходство в межъязыковом обучении. Используя общие базовые структуры различных языков, эти модели могут обобщать знания и

хорошо справляться с задачами, выходящими за рамки различных языковых границ [3].

Поскольку область языковых моделей LLM продолжает развиваться, такие проблемы, как интерпретируемость модели, эффективность данных и масштабируемость, остаются в центре внимания исследователей. Кроме того, ведутся работы по совершенствованию процесса тонкой настройки и улучшению компромисса между размером модели, вычислительными требованиями и экологической устойчивостью.

ChatGPT - это усовершенствованная языковая модель на основе архитектуры GPT-3.5, разработанная OpenAI. Она предназначена для ведения диалогов и предоставления информативных и контекстуально релевантных ответов на запросы пользователей. ChatGPT работает на основе комбинации методов глубокого обучения, массивного предварительного обучения на различных наборах данных и тонкой настройки на конкретных задачах [4].

В своей основе ChatGPT использует архитектуру нейронной сети-трансформера. Трансформаторы известны своей способностью улавливать дальние зависимости в последовательностях данных, что делает их особенно подходящими для задач обработки естественного языка. Эта архитектура состоит из нескольких слоев механизмов самовнимания, которые позволяют модели оценивать важность различных слов или лексем в заданном контексте.

Процесс обучения ChatGPT включает два основных этапа: предварительное обучение и тонкую настройку. Во время предварительного обучения модель подвергается воздействию огромного количества текстов из интернета, что позволяет ей изучить статистические закономерности, грамматику и знания о мире, присутствующие в данных. На этом этапе обучения без надзора используются такие методы, как моделирование языка по маске, когда определенные слова случайным образом маскируются, а перед моделью ставится задача предсказать их на основе окружающего контекста.

После завершения предварительного обучения проводится тонкая настройка на конкретных наборах данных, чтобы адаптировать модель к конкретным задачам или областям. Это предполагает обучение модели на более узком наборе данных с примерами, сгенерированными человеком, и обратной связью. Например, модель ChatGPT может быть доработана на наборах данных разговорной речи для улучшения ее разговорных способностей и генерации более контекстуально релевантных ответов.

В процессе вывода, когда пользователь взаимодействует с ChatGPT, входной запрос маркеризируется и проходит через уровни модели. Каждый токен обрабатывается параллельно, что позволяет

модели улавливать зависимости между различными частями входного запроса. Затем модель генерирует распределение вероятности по словарному запасу для предсказания следующей лексемы на основе предшествующего контекста. Этот процесс повторяется итеративно, чтобы сгенерировать ответ, последовательный и релевантный введенному запросу.

Важно отметить, что ответы ChatGPT основаны на шаблонах и информации, полученной в процессе обучения. Хотя модель стремится генерировать точные и полезные ответы, иногда она может выдавать неправильные или бессмысленные результаты. Кроме того, ChatGPT может быть чувствительна к формулировкам ввода и иногда проявлять предвзятость, присутствующую в обучающих данных. OpenAI продолжает работать над устранением этих ограничений и улучшением общей производительности модели.

В целом, ChatGPT работает благодаря сочетанию архитектуры трансформатора, предварительного обучения на больших наборах данных и тонкой настройки на конкретных задачах. Используя эти методы, ChatGPT способен участвовать в человекоподобных беседах и предоставлять информативные и контекстуально релевантные ответы на запросы пользователей.

В заключение следует отметить, что языковые модели LLM добились значительных успехов в понимании и создании естественного языка. Благодаря своей способности обучаться на огромных объемах данных, адаптироваться к различным областям и демонстрировать впечатляющие лингвистические способности, языковые модели LLM способны определить будущее обработки естественного языка, позволяя создавать преобразующие приложения в различных отраслях и сферах.

Список использованных источников:

1. Alberts I.L. et al. Large language models (LLM) and ChatGPT: what will the impact on nuclear medicine be? // European journal of nuclear medicine and molecular imaging. – 2023. – С. 1-4.

2. What are large language models and how do they work? // Boost AI: [Electronic resource] – Access mode: https://www.boost.ai/blog/llms-large-language-models#:~:text=At%20their%20core%2C%20large%20language,connections%20between%20words%20and%20phrases (Access date: 02.05.2023).

3. Lai V.D. et al. Chatgpt beyond english: Towards a comprehensive evaluation of large language models in multilingual learning //arXiv preprint arXiv: 2304.05613. – 2023.

4. Sabrina, Ortiz What is ChatGPT and why does it matter? Here's what you need to know / Ortiz Sabrina. // Zdnet: [сайт]. [Electronic resource] – Access mode: https://www.zdnet.com/article/what-is-chatgpt-and-why-does-it-matter-heres-everything-you-need-to-know/ (Access date: 05.05.2023).


КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ СОВРЕМЕННЫХ ВЫЗОВОВ
ҚАЗІРГІ ЗАМАНҒЫ СЫН-ҚАТЕРЛЕР ЖАҒДАЙЫНДАҒЫ КИБЕРҚАУІПСІЗДІК
CYBERSECURITY IN THE CONTEXT OF MODERN CHALLENGES

УДК 343.98

Вехов Виталий Борисович
Профессор кафедры Безопасность в цифровом мире Московского государственного технического университета имени Н.Э. Баумана (научно-исследовательского университета), доктор юридических наук, профессор, академик Российской академии естествознания (РАЕ), Заслуженный деятель науки и образования РАЕ,
г. Москва, Российская Федерация

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОГО ХАРАКТЕРА, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ «ДАРКНЕТ»

Аннотация. С учетом современной правоприменительной практики, базируясь на данных Государственного единого статистического учета о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании и прокурорском надзоре в Российской Федерации в статье рассмотрены актуальные теоретико-прикладные проблемы первоначального этапа расследования преступлений экстремистского характера, совершенных с использованием технологий «Даркнет». На основе анализа действующего законодательства автором приводятся выводы и предложения по совершенствованию квалификации и организации расследования преступных посягательств данного вида, в том числе взаимодействия следователя с сотрудниками специализированного органа дознания, по линии Интерпола и с уполномоченными лицами правоохранительных органов государств – участников Содружества Независимых Государств.

Ключевые слова: экстремизм в Интернете; квалификация преступлений экстремистского характера; планирование расследования; взаимодействие; экстремизм с использованием Даркнет.

Аннотация. Қазіргі заманғы құқық қолдану практикасын ескере отырып, қылмыстың жай-күйі туралы Мемлекеттік бірыңғай статистикалық есепке алу деректеріне, сондай-ақ Ресей Федерациясындағы қылмыстар, тергеу жұмыстары, тергеу және прокурорлық қадағалау туралы мәліметтерге сүйене отырып, мақалада «Даркнет» технологияларын қолдана отырып жасалған экстремистік сипаттағы қылмыстарды тергеудің бастапқы кезеңінің өзекті теориялық және қолданбалы мәселелері қарастырылған. Қолданыстағы заңнаманы талдау негізінде автор осы түрдегі қылмыстық қол сұғушылықтардың біліктілігін жетілдіру және тергеуді ұйымдастыру, оның ішінде тергеушінің мамандандырылған анықтау органының қызметкерлерімен, Интерпол желісі бойынша және Тәуелсіз Мемлекеттер Достастығына қатысушы мемлекеттердің құқық қорғау органдарының уәкілетті тұлғаларымен өзара іс-қимылы бойынша қорытындылар мен ұсыныстар береді.

Түйінді сөздер: Интернеттегі экстремизм; экстремистік сипаттағы қылмыстардың біліктілігі; тергеуді жоспарлау; өзара әрекеттесу; Даркнет қолдану арқылы экстремизм.

Annotation. Taking into account modern law enforcement practice, based on the data of the State Uniform Statistical Record on a condition of criminality, and also about reports of crimes, investigatory work, inquiry and prosecutorial supervision in the Russian Federation in article actual theoretical and applied problems of an initial stage of

investigation of crimes of extremist character made with use of "Darknet" technologies are considered. On the basis of the analysis of the current legislation the author gives conclusions and suggestions on improvement of qualification and organization of investigation of criminal encroachments of this type, including interaction of the investigator with employees of specialized body of inquiry, through Interpol and with the authorized persons of law enforcement bodies of the states - participants of the Commonwealth of Independent States.

Keywords: extremism on the Internet; qualification of extremist crimes; investigation planning; interaction; extremism using the Darknet.

По данным официальной уголовной статистики, в 2022 году в Российской Федерации было зарегистрировано – 522065 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Из них тяжкие и особо тяжкие преступные деяния составили 52%. С использованием сети Интернет, в том числе технологий «Даркнет», было совершено 73% преступлений. При этом было раскрыто всего 27% таких преступлений. Также следует подчеркнуть, что количество публичных призывов к осуществлению экстремистской деятельности, совершенных с использованием названных технологий, увеличилось на 8,4%, а выявление лиц, их совершивших, уменьшилось на 13,7% по сравнению с 2021 годом [1]. Из общего числа совершенных преступных деяний экстремистской направленности 66% составляют преступления рассматриваемой в настоящей статье категории [2]. Их раскрытие и расследование сопряжено с рядом трудностей, из которых наиболее значимыми, по нашему мнению, являются:

- отсутствие у сотрудников органов предварительного расследования знаний правового режима функционирования информационных ресурсов названного вида и, как следствие, проблематичность уголовно-правовой квалификации преступных деликтов выделенного вида;
- специфичность механизма следообразования, обусловленного применением специального программного обеспечения, работающего на основе алгоритмов криптографического преобразования информации и разных схем обмена данными в сети Интернет, условно называемых «анонимайзерами»;
- высокая степень защиты пользователей, работающих в сети Интернет по технологиям «Даркнет», от их идентификации (установления личности) правоохранительными органами;
- проблематичность установления места преступления и определения в связи с этим территориальности предварительного расследования и подсудности;
- недостаточное знание сотрудниками органов предварительного следствия и дознания международных договоров и соглашений о сотрудничестве в борьбе с преступлениями экстремистского характера,

совершенными с использованием информационных технологий; действующего законодательства в сфере информации, информационных технологий, связи и защиты информации; функций и возможностей специализированного органа дознания, а также Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора); особенностей получения, оценки и использования специфичных цифровых доказательств; правил формулирования вопросов специалистам и экспертам в области компьютерно-технических исследований и экспертиз.

Исследуем названные проблемы подробнее.

В соответствии с п. 4) ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) информационно-телекоммуникационная сеть Интернет представляет собой технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. При этом действия, направленные на получение информации определенным кругом лиц или ее передача такому кругу лиц считается предоставлением информации (п. 8) ст. 2 Закона об информации), а действия, направленные на ее получение неопределенным кругом лиц или ее передача этому кругу лиц квалифицируется как распространение информации (п. 10) ст. 2 Закона об информации).

С учетом изложенного, под распространением материалов экстремистского характера понимается незаконное предоставление конкретным лицам либо неопределенному кругу лиц возможности их использования посредством программного обеспечения, работающего по технологиям «Даркнет», например, путем направления электронного сообщения, автоматической их рассылкой определенному или неопределенному кругу лиц, размещения материалов на странице сайта, а также в виде ссылок для загрузки (скачивания) файлов с интернет-ресурсов, содержащих данные материалы.

Публичная их демонстрация будет заключаться в открытом показе либо в предоставлении неограниченному числу лиц возможности их просмотра без возможности самостоятельного их использования (путем сохранения на своем компьютерном устройстве, размещения на интернет-страницах от своего имени и т.п.). Как публичная демонстрация подлежат квалификации действия, совершенные в прямом эфире (в частности, на сайтах, позволяющих пользователям производить потоковое вещание), а также состоящие в размещении запрещенной законом информации (материалов, сведений) на личных страницах и на страницах групп пользователей (в социальных сетях или на интернет-страницах) [3; п. 22].

По мнению специалистов, около 90% всех информационных ресурсов, находящихся в сети Интернет, в настоящее время обрабатывается с использованием технологий «Даркнет» [4].

Рассматривая специфичность механизма цифрового следообразования по делам о преступлениях выделенной категории нельзя не отметить, что он обусловлен особенностями функционирования технологий «Даркнет». Базируясь на правовом понятии, изложенном в п. 2) ст. 2 Закона об информации, определим их как процессы и методы поиска, сбора, хранения, обработки, предоставления, распространения и защиты информации в сети Интернет, а также способы осуществления таких процессов и методов, основанные на использовании специализированного программного обеспечения. Оно применяется для сохранения анонимности и приватности действий, совершаемых в сети Интернет. С криминалистических позиций его представляется возможным классифицировать на следующие виды:

1. Поисковые системы (интернет-браузеры), например, такие как Tor (сокр. от англ. The Onion Router) [5] и I2P (от англ. Invisible Internet Project, IIP, I2P – проект «Невидимый интернет») [6].

2. Операционные системы типа Whonix [7], Subgraph [8], Tails [9].

3. Облачные хранилища данных, например Freenet [10].

Продолжая исследование выделенной дефиниции, отметим, что в трасологии используется достаточно устоявшееся понятие «дорожка следов» – система следов ног человека, состоящая из нескольких последовательно расположенных отпечатков обуви, ног, одетых в чулки или носки, а также босых ног. Известно, что эта система следообразования имеет присущие ей элементы. Данный термин употребляется и в одорологии для обозначения запахового следа преступника, который остается по пути его следования к месту преступления и от него. Именно по нему розыскная собака, используемая как биологический детектор, и ведет инспектора-кинолога, принимающего участие в розыске и задержании преступника «по горячим следам». На основании отмеченного методологического подхода, нами было предложено ввести в криминалистический оборот термин «дорожка электронных следов», которая представляет собой систему образования следов в сети Интернет, состоящую из нескольких последовательно расположенных по времени и логически взаимосвязанных записей о прохождении компьютерной информации по линиям связи через коммутационное оборудование оператора(-ов) связи и(или) провайдеров услуг Интернет от компьютера преступника до компьютера потерпевшего или в обратном порядке (в зависимости от следственной ситуации). Для получения максимально полной доказательственной информации о событии преступления, его участниках и причинно-следственных связях нами были выделены и с

применением метода «Timeline» исследованы элементы этой дорожки [11].

Для обеспечения качественного обнаружения, правильной процессуальной фиксации, полноценного предварительного и судебно-экспертного исследования, а также последующего использования специфических следов и доказательств целесообразно использовать по делам о преступлениях выделенного вида помощь специалистов в области цифровой криминалистики и судебных компьютерно-технических экспертиз. О существующих в настоящее время проблемах, связанных с их подготовкой и участием в уголовном судопроизводстве, мы писали ранее [12, 13].

Принимая за основу правовое положение лиц, осуществляющих оборот информации в сети Интернет и обладающих соответствующими правами и обязанностями, а также роль, которую они играют в раскрытии и расследовании преступлений экстремистского характера, совершенных с применением технологий «Даркнет», с криминалистических позиций представляется возможным классифицировать их на следующие категории:

1. Обладатели информации экстремистского характера – лица, самостоятельно создавшие такую информацию (п. «5) ст. 2. Закона об информации).

2. Владельцы сайтов и страниц сайтов, на которых находится информация названного вида – это лица, которые самостоятельно и по своему усмотрению определяют порядок использования сайтов и их страниц в компьютерной сети, в т.ч. порядок размещения на них такой информации (п. 17) ст. 2. Закона об информации).

3. Организаторы распространения информации экстремистского характера в компьютерной сети – лица, осуществляющие деятельность по обеспечению функционирования информационных систем и (или) программ для ЭВМ, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений, содержащих информацию рассматриваемого вида (п. 1 ст. 10.1. Закона об информации).

4. Владельцы новостных агрегаторов, с помощью которых осуществляется накопление и распространение информации экстремистского характера – владельцы программ для ЭВМ, сайтов и (или) страниц сайтов, которые используются для обработки и распространения новостной информации экстремистского характера, доступ к которым в течение суток составляет более одного миллиона пользователей (п. 1 ст. 10.4. Закона об информации).

5. Владельцы аудиовизуального сервиса, содержащего информацию экстремистского характера – владельцы сайтов и (или) страниц сайтов, и (или) информационных систем, и (или) программ для ЭВМ, которые используются для формирования и (или) организации

распространения в компьютерной сети совокупности аудиовизуальных произведений, содержащих информацию экстремистского характера, доступ к которым предоставляется за плату и (или) при условии просмотра рекламы, направленной на привлечение внимания потребителей, и доступ к которым в течение суток составляет более ста тысяч пользователей компьютерной сети (п. 1 ст. 10.5. Закона об информации).

6. Владельцы социальных сетей, обеспечивающих предоставление и (или) распространение информации экстремистского характера – владельцы сайтов и (или) страниц сайтов, и (или) информационных систем, и (или) программы для ЭВМ, которые предназначены и (или) используются их пользователями для предоставления и (или) распространения посредством созданных ими персональных страниц информации экстремистского характера, на которых может распространяться реклама данного вида преступной деятельности, направленная на привлечение внимания к ней, и доступ к которым в течение суток составляет более пятисот тысяч пользователей компьютерной сети (п. 1 ст. 10.6. Закона об информации).

7. Владельцы сервисов размещения объявлений, содержащих информацию экстремистского характера – владельцы сайтов и (или) страниц сайтов и (или) информационных систем и (или) программы для ЭВМ, которые предназначены и (или) используются для организации взаимодействия их пользователей между собой в целях купли-продажи, мены и (или) передачи в пользование движимого и (или) недвижимого имущества, выполнения работ, оказания услуг, поиска работы и (или) подбора лиц, обеспечивающих экстремистскую деятельность, за счет предоставления их пользователям возможности самостоятельно размещать объявления, тематически сгруппированные в зависимости от их содержания, а также за счет предоставления пользователям возможности самостоятельно обращаться по таким объявлениям и доступ к которым в течение суток составляет более ста тысяч пользователей сети (п. 1 ст. 10.7. Закона об информации).

8. Владельцы информационных ресурсов, содержащих информацию экстремистского характера, объем аудитории которых подлежит исследованию (п. 4 ст. 12.2. Закона об информации).

Для признания наличия в действиях подозреваемого (обвиняемого) признака совершения преступления экстремистского характера с использованием технологий «Даркнет» не имеют значения количество компьютерных устройств, работающих в сети Интернет по технологиям «Даркнет». При этом к числу таких компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны,

смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом [3; п. 2]. Обработанная таким образом информации экстремистского характера приобретает форму компьютерной информации, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (прим. 1 к ст. 272 УК РФ). Такие сведения могут находиться в оперативной памяти компьютерных устройств, на любых встроенных и внешних электронных носителях информации, и (или) передаваться по каналам электрической связи.

При квалификации преступных деяний рассматриваемого вида под сайтом, работающем по технологиям «Даркнет», следует понимать совокупность программ для компьютерных устройств и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством этой сети по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать такие сайты (п. «13)» ст. 2 Закона об информации). При этом интернет-страница представляет собой часть сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта (п. 14) ст. 2 Закона об информации). Доменное имя – это обозначение символами, предназначенное для адресации сайтов в сети в целях обеспечения доступа к информации, которая в ней размещена (п. 15) ст. 2 Закона об информации), а сетевой адрес есть идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему (п. 16) ст. 2 Закона об информации).

При определении места совершения преступлений выделенного вида и соответственно, решения вопроса о территориальной подследственности уголовного дела, необходимо учитывать, что доступ к сети Интернет, в том числе по технологии «Даркнет», может осуществляться с помощью различных мобильных компьютерных устройств. Местом совершения такого преступления будет являться место совершения лицом действий, входящих в объективную сторону состава преступления. Например, при публичных призывах к осуществлению экстремистской деятельности это будет территория, помещение или транспортное средство, где преступником использовался сотовый радиотелефон для направления другому лицу электронного сообщения, содержащего такие призывы, независимо от места нахождения другого лица, или использовался планшетный

компьютер для получения из информационных ресурсов, работающих по технологии «Даркнет», информации экстремистского характера с последующей ее массовой рассылкой определенному кругу лиц [3; п. 19].

Практика показывает, что возбуждению уголовного дела о преступлении рассматриваемой категории, как правило, предшествует предварительная проверка материалов, поступивших в правоохранительные органы. В этой связи следователь может заблаговременно ознакомиться с собранными по делу материалами, совместно с оперативными сотрудниками специализированного органа дознания – Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий МВД России (УБК МВД России) [14] выбрать в тактическом отношении наиболее оптимальный момент для возбуждения дела, а также определить характер и последовательность первоначальных следственных действий, оперативно-розыскных и организационных мероприятий.

Для оптимизации работы на данном этапе представляется целесообразным составление плана предварительной (доследственной) проверки поступивших материалов. В нем должны быть отражены следующие позиции:

- истребование необходимых материалов (документов), свидетельствующих о противоправности события;
- анализ полноты комплекта и содержания документов, подтверждающих противоправность исследуемого деяния;
- проверка подлинности и действительности документов, имеющихся в распоряжении органа предварительного расследования;
- вопросы лицам, на которые ссылается заявитель или имеются данные о них как о возможных свидетелях происшедшего события;
- получение объяснения от заявителя и возможных свидетелей (очевидцев) события;
- предварительное исследование содержания информации, предположительно имеющей экстремистский характер, с получением соответствующего письменного документа – заключения специалиста или специалистов в области лингвистики, психологии и лингвистики, религиоведения, культурологии, психологии и этнологии и др.;
- консультации со специалистами;
- ознакомление с информационным ресурсом, функционирующим в сети Интернет по конкретной технологии «Даркнет», с помощью которого было совершено преступление;
- изучение правового статуса пользователя (владельца) информационного ресурса, функционирующего в сети Интернет по конкретной технологии «Даркнет», с помощью которого было совершено преступление, установление его сетевого и юридического адресов;

- поиск сведений о владельце информационного ресурса рассматриваемого вида в находящихся в свободном доступе в сети Интернет Реестре организаторов распространения информации в сети Интернет (https://97-fz.rkn.gov.ru/), Реестре новостных агрегаторов (https://208-fz.rkn.gov.ru/), Реестре аудиовизуальных сервисов (https://87-fz.rkn.gov.ru/), Реестре социальных сетей (https://530-fz.rkn.gov.ru/), Реестре сервисов размещения объявлений (https://rkn.gov.ru/register-ord/register/), Реестре информационных ресурсов, объем аудитории которых подлежит исследованию (https://rkn.gov.ru/mass-communications/p856/), Едином реестре доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты, содержащие информацию, распространение которой в Российской Федерации запрещено (https://eais.rkn.gov.ru/) [15];

- направление запроса провайдеру хостинга – лицу, оказывающему услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет (п. 18) ст. 2 Закона об информации), оператору связи [16] или организатору распространения информации в сети Интернет [17] для установления пользователя (владельца) информационного ресурса, с помощью которого было совершено преступление;

- направление запроса в правоохранительный орган зарубежного государства об оказании правовой помощи по уголовным делам о преступлениях исследуемого вида в установлении отдельных обстоятельств происшедшего события и причастных к нему лиц.

Относительно последнего положения отметим следующее.

В рамках информационного обеспечения борьбы с преступлениями рассматриваемого вида от правоохранительных органов иностранных государств – членов Интерпола по соответствующим запросам может быть получена информация: а) о сетевых адресах, именах доменов и серверов организаций и пользователей; б) о содержании протоколов, трейсингов, логических файлов; в) об электронной информации, заблокированной в порядке оперативного взаимодействия правоохранительных органов при пресечении трансграничных правонарушений; г) о провайдерах и дистрибьюторах сетевых и телекоммуникационных услуг; д) о физических и юридических лицах, имеющих отношение к преступлениям названного вида [18; п. 96-97].

В соответствии с Соглашением о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий компетентные органы Сторон осуществляют сотрудничество в борьбе с распространением с использованием сети Интернет или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими [19].

Запрос направляется в письменной форме. В безотлагательных случаях запросы могут передаваться с использованием технических средств связи или устно, однако после этого в течение 3 суток они должны быть подтверждены письменно.

Запрос и материалы исполненного запроса могут передаваться по техническим каналам связи в случае, если об этом есть двусторонняя договоренность между компетентными органами Сторон либо эти каналы определены иными международными договорами, участниками которых являются Стороны.

Запрос должен содержать: а) наименование компетентного органа запрашивающей Стороны и компетентного органа запрашиваемой Стороны; б) изложение существа дела; в) указание цели и обоснование запроса; г) содержание запрашиваемого содействия; д) желательные сроки исполнения запроса; е) любую другую информацию, которая может быть полезна для исполнения запроса, включая соответствующие документы или их заверенные копии; ж) ссылку на настоящее Соглашение.

Запрос, переданный или подтвержденный в письменной форме, подписывается:

а) руководителем запрашивающего компетентного органа или его заместителем и скрепляется гербовой печатью компетентного органа - в случае если обмен информацией осуществляется между непрофильными подразделениями компетентных органов;

б) руководителем самостоятельного центрального профильного подразделения компетентного органа и скрепляется гербовой печатью самостоятельного центрального профильного подразделения компетентного органа – в случае если обмен информацией осуществляется между самостоятельными профильными подразделениями компетентных органов.

При исполнении запроса применяется законодательство запрашиваемой Стороны.

Список использованных источников:

1. Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации // Состояния преступности в Российской Федерации за январь – декабрь 2022 года. – М.: ФКУ «Главный информационно-аналитический центр», 2023. – С. 30 – 31.

2. В Генпрокуратуре России рассказали, где чаще всего совершаются экстремистские преступления. [Электронный ресурс] – Режим доступа: https://tass.ru/obschestvo/11854929 (дата обращения 06.04.2023).

3. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»».

4. Что такое глубокий и теневой интернет. [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/resource-center/threats/deep-web (дата обращения 06.04.2023).
5. Как работает Tor. [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/357128/ (дата обращения 06.04.2023).
6. Общее введение в I2P. [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/552072/ (дата обращения 06.04.2023).
7. Whonix: руководство для начинающих. [Электронный ресурс] – Режим доступа: https://habr.com/ru/company/alexhost/blog/532980/ (дата обращения 06.04.2023).
8. Защищенный Linux-дистрибутив Subgraph-OS: что внутри. [Электронный ресурс] – Режим доступа: https://xakep.ru/2016/10/20/subgraph-os/ (дата обращения 06.04.2023).
9. Tails OS или как защитить себя в сети. [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/439716/ (дата обращения 06.04.2023).
10. Опыт использования Freenet. [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/253127/ (дата обращения 06.04.2023).
11. Дорожка электронных следов как объект криминалистического исследования // Криминалисты Казахстана на службе правосудия: мат-лы международ. науч.-практ. конф. / под общ. ред. канд. юрид. наук доцента А. Дарменова. – Караганда: Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, 2019. – С. 15-20. – На казахском и русском языках.
12. Вехов В.Б. Опыт подготовки специалистов в области электронной криминалистике // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития. Материалы Международной научно-практической конференции 17 октября 2019 г. / Под общ. ред. А.М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019. – С. 126-128.
13. Вехов В.Б. Опыт подготовки специалистов в области судебных компьютерно-технических исследований и экспертиз // Фундаментальные и прикладные исследования в сфере судебно-экспертной деятельности и ДНК-регистрации населения Российской Федерации: материалы Всероссийской научно-практической конференции с международным участием 17-18 октября 2019 г. – Уфа: РИЦ БашГУ, 2019. – С. 59-62.
14. Приказ МВД России от 29.12.2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации».
15. Постановление Правительства Российской Федерации от 26.10.2012 № 1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено».
16. Постановление Правительства Российской Федерации от 27.08.2005 № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность».
17. Постановление Правительства Российской Федерации от 31.07.2014 № 759 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети Интернет информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного

текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети Интернет и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации».

18. Инструкция по организации информационного обеспечения сотрудничества по линии Интерпола // Приказ МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России, ФТС России от 06.10.2006 № 786/310/470/454/333/971 «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола».

19. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (утв. Советом глав государств СНГ 28.09.2018, Душанбе).

УДК 004.8: 343.721

Ефимов Сергей Владимирович
Управляющий партнер АНО Экспертно-правовой центр
«Финансовые расследования и судебные экспертизы»,
кандидат экономических наук,
г. Москва, Российская Федерация

Чернов Павел Леонидович
Управляющий партнер АНО Экспертно-правовой центр
«Финансовые расследования и судебные экспертизы»,
кандидат юридических наук,
г. Москва, Российская Федерация

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ АНАЛИЗЕ БОЛЬШИХ ДАННЫХ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ КОРПОРАТИВНЫМ МОШЕННИЧЕСТВАМ

Аннотация. Совершаемые мошенничества в компании весьма латентны, они скрыты в большом количестве учетной и иной информации. В связи с чем, их выявление достаточно трудоемко. На первое место выходит успешная автоматизация этих процессов. Учитывая закономерности отражения мошеннических схем в учетной информации, можно настроить достаточно эффективную систему их своевременного выявления, используя работу с большими данными.
Ключевые слова: корпоративные мошенничества; красные флажки; big data; автоматизация; хищения; коррупция; фальсификация отчетности.

Аннотация. Кәсіпорында жасалған алаяқтық өте жасырын болып табылады, олар бухгалтерлік және басқа ақпараттардың үлкен көлемде жасырылады. Нәтижесінде оларды анықтау өте қиын. Бұл процестерді сәтті автоматтандыру бірінші орында. Бухгалтерлік ақпаратта жалған схемаларды көрсету заңдылықтарын ескере отырып, үлкен деректерді пайдалана отырып, оларды дер кезінде анықтаудың жеткілікті тиімді жүйесін құруға болады.
Түйінді сөздер: корпоративтік алаяқтық; қызыл жалаулар; үлкен деректер; автоматтандыру; ұрлық; сыбайлас жемқорлық; бұрмаланған есеп беру.

Annotation. Frauds committed in the company are very latent, they are hidden in a large amount of accounting and other information. As a result, their detection is quite difficult. Successful automation of these processes comes first. Taking into account the patterns of reflection of fraudulent schemes in accounting information, it is possible to set up a fairly effective system for their timely detection using big data.
Keywords: corporate fraud; red flags; big data; automation; theft; corruption; falsified reporting.

Противодействие мошенническим действиям предполагает предметную подготовку, требующую больших временных и трудовых ресурсов для доказывания.

Из статистики уголовных правонарушений за 2022 год, публикуемой Органами правовой статистки и специальных учетов Генеральной прокуратуры Республики Казахстан (КПСиСУ), следует, что число регистрируемых фактов мошенничества (ст. 190 УК РК) с каждым годом увеличивается [1].

Согласно классической теории, поводом для возникновения мошеннических действий являются три условия: необходимость (motive), возможность (opportunity) и обоснование (rationalization). Это так называемый «треугольник мошенничества» Дональда Кресси (Donald Cressey's Fraud triangle) [2].

Научные исследования засвидетельствовали, что каждые трое из десяти работников ищут возможности что-либо украсть, другие трое из десяти украдут, как только представится такая возможность, и лишь четверо из десяти останутся честными при любых обстоятельствах [3].

В соответствии с деревом корпоративного мошенничества существует три элемента мошенничества: хищения, коррупция, фальсификация отчетности [4]. Причем мошенничества в форме хищения совершаются в отношении денежных средств, основных средств и материалов, а также прочих активов. Кроме этого, согласно дереву корпоративного мошенничества, фальсификация отчетности и хищение активов тесно взаимосвязаны при реализации задач по сокрытию следов противоправных деяний. Это не отменяет наличие в регистрах бухгалтерского учета «аномалий», выраженных в несвойственных для компании операциях и результатов их отражения.

Чем быстрее вы выявите подозрительную аномалию, чем ближе на временной оси вы будете к факту совершения мошенничества, тем выше будет эффективность работы системы борьбы с мошенничеством в целом.

Все истории длительного безнаказанного масштабного мошенничества в первую очередь основаны на отсутствии быстрого реагирования на такие аномалии.

Данное обстоятельство свидетельствует о возникновении индикаторов корпоративного мошенничества, выявление которых реализуемо с применением новейших методов обработки информации.

Путем грамотного осуществления сбора, анализа и систематизации фактов, имеющих доказательственное значение в результате обнаружения признаков экономических преступлений, можно эффективно раскрывать противоправные действия персонала и связанных с ним лиц.

Существенно облегчить выявление данных аномалий можно с использованием различных программных продуктов на основании заложенных алгоритмов по поиску информации внутри бухгалтерского учета компании с помощью технологий обработки больших данных. В перспективе, с развитием машинного обучения, возможна разработка

алгоритмов самим программным комплексом (искусственным интеллектом) на основе анализа массива данных.

Технология Big Data – метод обработки большего числа данных для получения новой информации. Анализ огромного количества сведений обычными способами, то есть путем осмотра и ручного вычленения необходимых данных для дальнейшего их изучения, труднореализуем, поскольку требует длительного времени и монотонной работы со стороны исследователей. Следовательно, применяющиеся технологии упрощают процесс анализа информации.

Технологии Big Data призваны автоматизировать анализ индикаторов риска на основе сканирования данных регистров бухгалтерского учета. Так, авторами разработана совокупность последовательных действий по выявлению аномалий, указывающих на возможное совершение мошеннических действий в отношении имущества организации. К примеру, при хищении товарно-материальных ценностей (далее – ТМЦ) формируются остатки на счетах учета товаров, материалов, готовой продукции, которые впоследствии списываются на счет учета недостач. При росте остатков или увеличении недостач возникают основания полагать, что имеет место совершение необоснованных операций в отношении имущества организации. Ниже приведены категории схем хищений (таблица 1), имеющих свои признаки при обработке сведений из регистров бухгалтерского учета.

Таблица 1

п/п	Категория	Схема совершения мошенничества
1	Схемы хищений и иных экономических преступлений в сфере закупок	1. Закупки по завышенной стоимости 2. Оплата за несуществующие товары, работы, услуги 3. Вознаграждения за выбор поставщика, предоставление ему льготных условий
2	Схемы хищений и иных экономических преступлений в сфере оприходования и хранения товарно-материальных ценностей	4. Списание ТМЦ под фиктивным предлогом
3	Схемы хищений и иных экономических преступлений в сфере производства, эксплуатации, строительства и ремонта	5. Подмена материалов, комплектующих в технологическом (строительном, ремонтном) процессе/фиктивное списание 6. Игра на измерении и оценке активов в производственном процессе 7. Завышение параметров в сметах и проектной документации
4	Схемы хищений и иных экономических преступлений с основными средствами	8. Отчуждение основных средств на заведомо невыгодных компании условиях 9. Фальсификация учетной и иной документации в целях хищения основных средств
5	Схемы хищений и иных экономических преступлений в сфере «начислений» (с участием	10. Мошенничество при начислении и выплате заработной платы и премий, выплаты дивидендов 11. Злоупотребления в сфере выплат, связанных с командировками

	финансовых и кадровых служб)	12. «Кредитование» через подотчетных лиц
6	Схемы хищений и иных экономических преступлений в сфере продаж	13. Неотражение продаж 14. Продажи с занижением цены (в том числе через подконтрольные фирмы) 15. Незаконное получение вознаграждения за предоставление покупателю льготных условий 16. Умышленное получение в оплату неликвида (дебиторская задолженность, нереальная к взысканию, неликвидные ценные бумаги) 17. Продажи нормальной продукции под видом брака или неликвида 18. Выдача заведомо невозвратного товарного кредита 19. Вывод клиентов
7	Схемы хищений и иных экономических преступлений в сфере займов и кредитов	20. Займы взаимозависимым лицам

Общая методика обнаружения схем хищений и других экономических преступлений заключается в сканировании регистров бухгалтерского учёта на предмет наличия в них выходящих за установленные (рекомендованные) нормы явлений. Автоматизацию обработки данных сведений следует производить на основе программного обеспечения, разработанного в целях реализации алгоритмов. Результатом обработки данным ПО сведений из регистров будет отображение конечных индикаторов мошеннических действий.

Далее приведены примеры способов хищений активов компании, в парадигме обнаружения их признаков технологиями Big Data.

Одной из самых подверженных риску областей учета является сфера оприходования и хранения товарно-материальных ценностей.

Списание ТМЦ под фиктивным предлогом – хищение, совершаемое персоналом, имеющим доступ к активам и возможность совершить их списание (подготовить документы на их списание). Первая фаза преступления – активы скрытно выносятся из компании самыми различными способами. Затем добавляется вторая фаза – сокрытие следов преступления. В данной схеме в качестве такой фазы выступает списание похищенных ТМЦ под обоснованным преступниками предлогом: усушка, утруска, стихийное бедствие, пожар, пересортица, хищение и т.д. Таким образом, в учете не образуются недостачи, и компания может длительное время и не подозревать о совершенном хищении.

Существует и обратная ситуация, когда происходит затоваривание в учете при фактическом выбытии товаров из компании. Например, при закупке ТМЦ за безналичный расчет и продажу за наличный без отражения в учете.

Не всегда признаки данных преступлений можно обнаружить простым способом. В частности, следует путем сплошного мониторинга

выявлять аномальные тенденции, такие как неоправданное увеличение на 10% и более за год остатков на счетах 41, 10, 20, 25, 26, 44.

К примеру, согласно оборотам счета 41 «Товары» в период с 2019 по 2021 гг. происходит рост товаров на складе: со 170 млн. руб. в 2019 г. до 308 млн руб. в 2020 г. (рост на 80% к 2019 г.) и до 791 млн руб. в 2021 г. (рост на 157 % к 2020 г.). Следовательно, при увеличении покупок обществом не происходит соответствующего роста реализации ТМЦ.

Примеры других индикаторов приведены в таблице 2.

Таблица 2.

Критерий	Счета б/у	Сумма	О чем свидетельствует	Как часто проводить
Выбытие ОС	01,90	от 1 млн руб.	Отчуждение основных средств на заведомо невыгодных компании условиях	не реже одного раза в квартал
Консультационные услуги	20,25,26	от 100 тыс. руб.	Вывод денежных средств	не реже одного раза в месяц
Увеличение остатков ТМЦ	10,41	на 10% и более за квартал	Выставление поставщиком счетов и оплата счетов за несуществующие товары, работы и услуги	не реже одного раза в квартал
Увеличение з/п	70,20,25, 26,51	на 10% и более за месяц	Мошенничество при начислении и выплате заработной платы и премий	не реже одного раза в месяц
Отнесение на недостачу	94,41,10	более 5% валюты баланса	Умышленная дефектная поставка; Списание ТМЦ под фиктивным предлогом; Игра на измерении и оценке активов в производственном процессе	не реже одного раза в месяц
Приобретение чужих векселей	58,76,51	более 5% валюты баланса	Умышленное получение в оплату за существующие/несуществующие товары/услуги/ работы неликвидных ценных бумаг Вывод денежных средств	не реже одного раза в месяц
Выдача векселей	60,76,51	более 5% валюты баланса	Установление дальнейшего использования денежных средств (возможность вывода средств через собственную компанию)	не реже одного раза в месяц
Распределение прибыли	84,75,51	более 5% валюты баланса	Предпочтительное (непропорциональное) распределение прибыли между участниками	не реже одного раза в квартал
Снижение д/с на расчетных счетах	51	на 30% по отношению к остатку на 1 число месяца	Неотражение продаж, вывод денежных средств по разным фиктивным основаниям (оплата за несуществующие товары/услуги/ работы и т.п.)	не реже одного раза в месяц
Снижение выручки	90.01, 62	на 30% по отношению предыдущему кварталу	Неотражение продаж; Продажи с занижением цены (в том числе через подконтрольные фирмы)	не реже одного раза в квартал
Остаток на счетах	25,26,44	наличие остатков по итогам года / отрицательные остатки	Подмена материалов, комплектующих в технологическом (строительном, ремонтном) процессе	не реже одного раза в год
Увеличение запасов при уменьшении кредиторской задолженности	41,60,51	на 10% и более за квартал (соответственно)	Умышленное получение в оплату неликвида Выставление поставщиком счетов и оплата счетов за несуществующие товары, работы и услуги Вывод денежных средств	не реже одного раза в квартал
Увеличение дебиторской задолженности	60,62,51	на 10% и более за квартал	Умышленное получение в оплату неликвида Вывод запасов/денежных средств	не реже одного раза в квартал
Рост себестоимости выше роста выручки	90.01, 90.02	на 10% за квартал	Продажи с занижением цены (в том числе через подконтрольные фирмы)	не реже одного раза в квартал
Выдача займов	58,51	более 5% валюты баланса	Вывод денежных средств	не реже одного раза в месяц

Критерий	Счета б/у	Сумма	О чем свидетельствует	Как часто проводить
Получение займов	66,67,51	более 5% валюты баланса	Установление дальнейшего использования денежных средств (возможность вывода средств через собственную компанию)	не реже одного раза в месяц
Увеличение выдачи д/с под отчет	71,51	более 5% валюты баланса	Злоупотребления в сфере выплат, связанных с командировками; «Кредитование» через подотчетных лиц Вывод денежных средств	не реже одного раза в месяц

Существует достаточно большое количество индикаторов в бухгалтерском учете, которые могут свидетельствовать о злоупотреблениях в компаниях. В случае выявления негативных закономерностей необходимо осуществлять дополнительную их проверку, в ходе которой далеко не всегда подтверждается наличие мошеннических действий. Вместе с тем автоматизация процедур контроля с использованием Big data, и в перспективе искусственного интеллекта, позволяет оперативно выявлять и реагировать на негативные процессы в компании, своевременно инициировать полноценное финансовое расследование и, как следствие, повышает вероятность успеха по раскрытию мошеннических схем.

Список использованных источников:

1. Официальный портал Органов правовой статистики и специальных учетов Генеральной прокуратуры Республики Казахстан. [Электронный ресурс] - Режим доступа: https://qamqor.gov.kz/ (дата обращения: 25.04.2023).

2. С. Альбрехт, Дж. Венц, Т. Уильямс. Мошенничество. Луч света на темные стороны бизнеса / Перев. с англ. – СПб. : Питер, 1995. С. 400.

3. W. Steve Albrecht. Iconic Fraud Triangle endures. [Электронный ресурс] - Режим доступа: https://www.fraud-magazine.com/article.aspx?id=4294983342 (дата обращения: 25.04.2023).

4. Occupational Fraud 2022: A Report to the Nation. [Электронный ресурс] - Режим доступа: https://legacy.acfe.com/report-to-the-nations/2022 (дата обращения: 25.04.2023).

УДК 343.3/.7:004

Кадырбеков Сагынбек Сейитбекович
Преподаватель кафедры Криминалистики и информационных технологий Академии МВД Кыргызской Республики,
старший лейтенант милиции,
г. Бишкек, Кыргызская Республика

ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И БОРЬБА С НИМИ

Аннотация. Статья исследует преступления в сфере информационных технологий и меры по их пресечению и преследованию. Рассматриваются различные аспекты преступлений в сфере информационных технологий: анализ типов и классификация киберпреступлений; исследование различных техник и методов атак, используемые злоумышленниками; выделены основные уязвимости информационных систем; предложены меры по их защите от киберпреступлений, а также подчеркивается важность обучения и повышения осведомленности пользователей об угрозах кибербезопасности. Автор статьи призывает к совместным усилиям государств, организаций и пользователей для создания безопасной и надежной среды в цифровом мире.

Ключевые слова: виды киберпреступлений; преступления в сфере информационных технологий; хакерство и несанкционированный доступ; кибершпионаж; фишинг; мошенничество; распространение вредоносных программ; кибертерроризм; анализ; активность; сложность; методы борьбы; защита данных.

Аннотация. Мақалада ақпараттық технологиялар саласындағы қылмыстар мен олардың жолын кесу және қудалау шаралары қарастырылған. Ақпараттық технологиялар саласындағы қылмыстардың әртүрлі аспектілері қарастырылады: киберқылмыстардың түрлері мен жіктелуін талдау; шабуылдаушылар қолданатын әртүрлі әдістер мен шабуыл әдістерін зерттеу; ақпараттық жүйелердің негізгі осал тұстары көрсетілген; оларды киберқылмыстан қорғау шараларын ұсынып, киберқауіпсіздік қатерлері туралы пайдаланушыларды оқыту мен хабардар етудің маңыздылығын атап өтті. Мақала авторы цифрлық әлемде қауіпсіз және қауіпсіз орта құру үшін мемлекеттердің, ұйымдардың және пайдаланушылардың бірлескен күш-жігерін біріктіруге шақырады.

Түйінді сөздер: киберқылмыс түрлері; ақпараттық технологиялар саласындағы қылмыстар; бұзу және рұқсатсыз кіру; кибер тыңшылық; фишинг; алаяқтық; зиянды бағдарламаларды тарату; кибертерроризм; талдау; белсенділік; күрделілік; күрес әдістері; деректерді қорғау.

Annotation. The article explores crimes in the field of information technology and measures to suppress and prosecute them. Various aspects of crimes in the field of information technology are considered: analysis of types and classification of cybercrimes; study of various techniques and methods of attacks used by attackers; the main vulnerabilities of information systems are highlighted; suggested measures to protect them from cybercrime, and stressed the importance of educating and raising user awareness of cybersecurity threats. The author of the article calls for joint efforts of states, organizations and users to create a safe and secure environment in the digital world.

Keywords: types of cybercrime; crimes in the field of information technology; hacking and unauthorized access; cyber espionage; phishing; fraud; distribution of malware; cyberterrorism; analysis; activity; complexity; methods of struggle; data protection.

Развитие информационных технологий привело к возникновению новых форм преступлений, связанных с компьютерами и сетями. Киберпреступность стала серьезной угрозой для государств, организаций и отдельных лиц, поэтому борьба с ней становится все более важной. На сегодняшний день, к основным видам киберпреступлений можно отнести**:**

1. Хакерство и несанкционированный доступ (несанкционированный доступ к компьютерным системам или сетям с целью кражи, разрушения или манипуляций с данными);
2. Кибершпионаж и кража данных (незаконное получение конфиденциальной информации, включая персональные данные, банковские реквизиты, коммерческие секреты или государственные секреты);
3. Фишинг и мошенничество (использование поддельных веб-сайтов или электронных сообщений для обмана пользователей с целью получения их личных данных или финансовых реквизитов);
4. Распространение вредоносных программ (создание и распространение вирусов, троянов, шпионского программного обеспечения и других вредоносных кодов с целью нанесения вреда компьютерным системам или кражи информации);
5. Кибертерроризм (использование информационных технологий для совершения террористических актов или кибератак на критическую информационную инфраструктуру) и т.д.

Борьба с вышеперечисленными видами киберпреступлений требует комплексного подхода и использования различных мер и инструментов, среди которых можно перечислить следующие:

1. Нормативно-правовое регулирование (разработка и принятие соответствующих законов, направленных на пресечение киберпреступности) [1; 2; 3];
2. Создание специализированных подразделений правоохранительных органов для расследования и преследования киберпреступников;
3. Использование современных методов шифрования, файрволлов и систем обнаружения вторжений от несанкционированного доступа;
4. Использование уникальных и сложных паролей, а также включение дополнительных методов аутентификации, таких как отпечатки пальцев или одноразовые коды, для повышения безопасности доступа к системам и аккаунтам;
5. Обучение пользователей основам кибербезопасности, чтобы они могли распознавать потенциальные угрозы и принимать

соответствующие меры предосторожности при работе с информацией и использовании онлайн-сервисов;

6. Регулярное обновление программного обеспечения (установка последних обновлений и патчей для операционных систем, приложений и антивирусных программ, чтобы исправить уязвимости и предотвратить эксплуатацию их злоумышленниками);

7. Мониторинг и обнаружение вторжений (использование специализированных систем обнаружения вторжений (Intrusion Detection Systems, IDS) и систем обнаружения вторжений в реальном времени (Intrusion Prevention Systems, IPS) для контроля сетевого трафика и обнаружения аномалий или подозрительной активности);

8. Резервное копирование данных (регулярное создание резервных копий данных и хранение их в безопасных местах для предотвращения потери информации в случае кибератаки или сбоя системы).

Вместе с тем, наряду с вышеуказанными мерами борьбы с киберпреступлениями, на мой взгляд, особое значение имеет международное сотрудничество, потому как киберпреступность не имеет границ и международное сотрудничество в борьбе с ней является необходимостью. Совместные усилия государств, международных организаций и частного сектора могут способствовать обмену информацией о новых угрозах, разработке общих стандартов безопасности и совместным расследованиям киберпреступлений. Так, 17 января 2023 года, в Вене была проведена четвертая сессия Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Где шла речь о киберпреступности, которая подрывает благополучие миллионов людей в мире и оборачивается серьезными экономическими потерями:

«Во многих национальных уголовных кодексах даются определения различных видов киберпреступлений – от кражи личных данных, средств из банков с использованием интернет–технологий до мошеннических сделок и т. д. Но даже если такое законодательство имеется, оно зачастую бывает разнородным и не совпадает по терминологии в силу специфики этих преступлений, а специфика такая, что преступление может произойти на территории одного государства, а ущерб может быть причинен на территории другого. Поэтому для целей сотрудничества между правоохранительными органами разных стран наилучший способ – это использование общей конвенции, которая будет унифицировать все эти составы преступлений.

Сегодня киберпреступность становится все более распространенной, а связанный с ней нелегальный оборот финансовых средств достигает триллионов долларов.

Террористические группировки и преступные организации активно пользуются «теневым интернетом», через который осуществляется

доступ к черным рынкам наркотиков и оружия. Мошенники воруют личные данные через интернет, а террористы вербуют новых бойцов в свои ряды и распространяют свою человеконенавистническую идеологию. Ни одна страна мира не может бороться с этими угрозами в одиночку.

В 2018 году ущерб от киберпреступности составил 1,5 трлн долларов в год. К 2025 году этот показатель может достичь уже девяти триллионов [4].

Кроме этого, Group-IB предупредила о главных киберугрозах 2023 года [5]. В Group-IB уверены, что в 2023 году империя программ-вымогателей сохранит лидерство в рейтинге киберугроз для бизнеса. Эксперты компании Group-IB опубликовали аналитический отчет "Эволюция киберпреступности: Анализ, тренды и прогнозы на 2022/2023, в котором обозначили основные киберриски для бизнеса. По данным Group-IB, империя программ-вымогателей будет в 2023 году находиться на первом месте в рейтинге киберугроз. Наиболее активными группами в 2022 году были Lockbit, Conti и Hive.

Специалисты компании отмечают, что структура киберпреступных группировок становится все сложнее и напоминает структуру легальных ИТ-стартапов. Ransomware-as-a-Service (RaaS) является основным двигателем развития индустрии шифровальщиков. Group-IB обнаружила 20 новых публичных партнерских программ в период с H2 2021 по H1 2022, из которых в 2023 году сохранятся только сильнейшие, мелкие группы будут распадаться, а их участники перейдут в более крупные.

Как сообщается в отчете, количество сайтов, где злоумышленники опубликовывают украденные данные компаний для более эффективного давления на жертв, называемых Dedicated Leak Sites (DLS), увеличилось на 83% за период H2 2021 - H1 2022 до 44 сайтов. По данным Group-IB, ежедневно на DLS появляются данные 8 жертв, атакованных шифровальщиками, и всего в публичном доступе были опубликованы данные 2 894 компаний.

В 2022 году данные, украденные с помощью стилеров, стали одним из трех самых продаваемых товаров в даркнете, наряду с доступами и текстовыми данными банковских карт (имя владельца, номер карты, срок истечения, CVV). Стилеры стали активно использоваться в атаках на корпорации в связи с ростом популярности удаленной работы и сервисов единого входа (SSO). На некоторых платформах такие программы раздаются «доброжелателями» даже бесплатно. По оценкам Group-IB, стилеры являются второй по значимости угрозой после шифровальщиков [6].

Геополитические события 2022 года внесли серьезные коррективы в характер киберпреступлений. Изменились мотивы злоумышленников, состав их участников и доступные им ресурсы. В связи с этим у бизнеса появилась необходимость расширять инструментарий прогнозирования

действий киберпреступников и разрабатывать стратегии и тактики проактивной защиты ИТ-инфраструктуры предприятий.

Основными наблюдаемыми трендами стали интенсификация DDoS-атак, изменения в инфраструктурах компаний, связанные с импортозамещением, продолжение активности программ-вымогателей, и все это на фоне критической нехватки квалифицированных кадров в области кибербезопасности. Давайте вместе посмотрим, как проактивная аналитика угроз может помочь справиться с этими вызовами.

Международная напряженность сохранится и в 2023 году, а значит, те проблемы, которые испытывали коммерческие и государственные компании останутся актуальными. Злоумышленники, мотивированные не только финансово, но и политически, будут пытаться нанести как можно больший ущерб отдельным учреждениям и критическим объектам промышленности и инфраструктуры. Улучшится координация атакующих групп. Вырастет сложность и изощренность атак, хотя и простые массовые атаки, направленные на отказ в обслуживании, никуда не исчезнут. В этой связи эффективным инструментом защиты могут стать инструменты Threat Intelligence (TI). Ранее процент атак, в которых удавалось детектировать атакующие узлы доходил до 80% в сутки, а предсказать удавалось до 8% атакующих узлов. Это означает, что для атаки интенсивностью 900 Gbps, за счет использования данных TI можно будет освободить трафик объемом около 70 Gbps, а это эквивалентно 16000 пользователей.

Более того, данные индикаторов, кроме самих индикаторов для блокировки (ip-адресов, атакуемых/атакующих портов), содержат дополнительную информацию. Например, о принадлежности адреса конкретному провайдеру, использовании этих адресов для вредоносной активности ранее, принадлежности к ботнет-сети и другую. Такие данные позволят осуществлять более сложную аналитику проводимой атаки, предсказать, какие инструменты может использовать потенциальный злоумышленник и на какие события информационной системы следует обратить более пристальное внимание.

Стали уходить иностранные вендоры, бизнесу перестали продавать продукты и лицензии, начали отказывать в предоставлении услуг и сервиса. Как следствие, возникла потребность в перестройке инфраструктуры, стали меняться подходы к ее защите. В свете этой тенденции свою эффективность в качестве универсального инструмента показал TI.

В условиях санкций и остановке работы зарубежных поставщиков компаниям пришлось искать альтернативу в виде отечественных продуктов с аналогичной функциональностью или обращаться к Open Source-решениям. С учетом санкционных рисков и вероятности блокировки доступа различных пользователей к репозиториям,

отсутствия гарантий в части наличия вредоносного кода в них, на последние не приходится делать больших ставок в долгосрочной перспективе. Так, в августе 2022 года исследователями были выявлены зараженные пакеты в репозитории pip (пакетный менеджер для Python), чем явно было продемонстрировано, что угрозу могут представлять даже те продукты, которые всегда считались доверенными. Разумеется, исследователи предоставили индикаторы компрометации, связанные со злонамеренно измененными пакетами, а значит, компании, использующие TI, будут защищены.

Простота и однозначность индикаторов, полученных от команд TI, позволяет создавать элементы защиты, не зависящие от особенностей конечных точек. При этом не важно, кто обратился к вредоносному ip-адресу: рабочая станция, телефон или умный чайник – обращение детектируется и уведомление об этом поступает офицеру безопасности. Таким образом, обнаружение основывается на знаниях о злоумышленнике и не обязано быть напрямую привязанным к особенностям динамически изменяющейся инфраструктуры защищающейся компании.

Сам по себе TI не заменяет сигнатурных методов обнаружения, но значительно расширяет возможности как уже развернутых, так и вновь приобретаемых средств защиты. Кроме того, для обеспечения актуального уровня безопасности в условиях доступа к данным с использованием не доверенных устройств требуется автоматизация и использование шаблонов реакции на события ИБ. Неоценимую помощь в этом случае оказывает уже упоминавшийся дополнительный контекст об угрозах, который предоставляется в рамках реализации процесса анализа киберугроз. Наличие в контексте информации о принадлежности к вредоносным или нежелательным объектам или наоборот легитимным сервисам позволяет создавать гибкие правила реагирования и даже реализовывать элементы проактивной защиты. Например, за счет знания собственных DNS-серверов компании (если компании, все же, удалось провести полноценную инвентаризацию) и списков «белых» DNS - серверов можно реализовать простой механизм контроля DNS-tunneling, при этом не мешая работе пользователей.

Затормозить рост развития шифровальщиков с помощью TI

Еще одной актуальной тенденцией остается рост атак с использование программ-вымогателей. Доступ к инструментам управления и распространения подобного вредоносного софта упрощается, порог вхождения для злоумышленника падает, а стоимость выкупа или желание парализовать работу информационного актива «под заказ» делают использование этого инструмента весьма привлекательным. Также ransomware используется и в атаках, инспирированных политическими событиями.

Согласно отчетам множества именитых игроков рынка кибербезопасности за 2022 год, от 12 до 20% всех атак на критическую инфраструктуру было совершено с использованием шифровальщиков. Реализация подобных атак стала значительно проще. Если раньше атаки совершались группами, которые и разрабатывали, и распространяли вредоносное ПО, то сейчас инструменты атак и управления зараженными узлами предоставляются как сервис, а термин RaaS (Ransomware as a Service) уже прочно вошел в употребление. Грубо говоря, для эксплуатации инструментов заражения и получения выкупа не обязательно обладать специальными навыками, достаточно заплатить. Причем конкуренция между поставщиками RaaS постоянно растет. Стоимость программ-вымогателей за последние 4 года по некоторым позициям снизилась с $300 до $10, но угроза реализации атак с использованием этого ПО по-прежнему остается одной из основных.

Использование злоумышленниками RaaS-модели позволяет отслеживать такие передающиеся «из рук в руки» управляющие сервера с помощью TI и оперативно добавлять их в списки индикаторов компрометации, что усиливает превентивную защиту на базе таких списков. Знания об особенностях атаки и методах ее реализации, которые так же могут поставляться в рамках сервиса анализа киберугроз, повышают эффективность мер реагирования на уже произошедшие инциденты, позволяя сократить площадь поражения [7].

Таким образом, необходимо отметить, что киберпреступность представляет серьезную угрозу для информационной безопасности в современном мире. Она может нанести значительный ущерб государствам, организациям и частным лицам. Однако применение эффективных мер по кибербезопасности и борьбе с киберпреступностью может существенно снизить риски и защитить информацию. Только через постоянную внимательность, обновление знаний и сотрудничество мы сможем создать безопасную информационную среду и минимизировать риски, связанные с киберпреступностью.

Список использованных источников:

1. Закон Кыргызской Республики "Об информации персонального характера" от 12 июля 2022 года № 61. [Электронный ресурс] – Режим доступа: http://cbd.minjust.gov.kg/act/view/ru-ru/112388?cl=ru-ru (дата обращения 1.04.2023 г.).

2. Постановление Правительства Кыргызской Республики от 3 мая 2019 года № 209 «Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы» [Электронный ресурс] – Режим доступа: http://cbd.minjust.gov.kg/act/view/ru-ru/13648 (дата обращения 1.04.2023 г.).

3. Постановление Правительства Кыргызской Республики от 24 июля 2019 года № 369 «Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы» [Электронный ресурс] – Режим доступа: http://cbd.minjust.gov.kg/act/view/ru-ru/15478 (дата обращения 2.04.2023 г.).

4. В Вене проходят переговоры по разработке конвенции о борьбе с киберпреступностью [Электронный ресурс] – Режим доступа: https://news.un.org/ru/story/2023/01/1436692 (дата обращения 2.04.2023 г.).

5. Group-IB предупредила о главных киберугрозах 2023 года [Электронный ресурс] – Режим доступа: https://www.securitylab.ru/news/535813.php?ref=123 (дата обращения: 5.04.2023 г.).

6. Эволюция киберпреступности: Анализ, тренды и прогнозы на 2022/2023 [Электронный ресурс] – Режим доступа: https://www.facct.ru/resources/research-hub/hi-tech-crime-trends-2022/ (дата обращения: 7.04.2023 г.).

7. Каковы тренды активности злоумышленников, которые сохранятся в 2023 году, и что необходимо знать о контексте киберугроз? [Электронный ресурс] – Режим доступа: https://www.it-world.ru/cionews/security%20/190929.html (дата обращения 07.04.2023 г.).

УДК 004.056.53:34

Лебедев Вадим Николаевич
Старший научный сотрудник отдела правовой статистики и информационного обеспечения прокурорской деятельности Университета прокуратуры Российской Федерации, кандидат технических наук, доцент, советник юстиции
г. Москва, Российская Федерация

К ВОПРОСУ О МЕСТЕ КИБЕРБЕЗОПАСНОСТИ В ГОСУДАРСТВЕННОЙ СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В статье кратко рассмотрены состояние и правовое регулирование понятия «кибербезопасность» в некоторых зарубежных странах и в Российской Федерации. Проанализированы определения понятия «кибербезопасность» содержащиеся в национальных правовых актах и международных документах, изучены подходы отдельных ученых и специалистов к трактовке данного понятия. Определены объекты защиты кибербезопасности исходя из взглядов разных стран на обеспечение кибербезопасности.

Проведен анализ функционального соотношения понятий «кибербезопасность» и «информационная безопасность», обоснован подход к их соотношению. На основе чего сделано заключение о возможности решения целей и задач кибербезопасности в рамках существующих подходов к обеспечению информационной безопасности в Российской Федерации и нецелесообразности правового регулирования кибербезопасности в стране.

Ключевые слова: информационная безопасность; кибербезопасность; информационно-телекоммуникационные сети; информационные технологии; информационная инфраструктура; объекты защиты; информационная безопасность Российской Федерации; обеспечение безопасности информации и информационных ресурсов; обеспечение безопасности информационной инфраструктуры; обеспечение безопасности от деструктивного информационно-психологического воздействия.

Аннотация. Мақалада кейбір шет елдерде және Ресей Федерациясында «киберқауіпсіздік» ұғымының жағдайы мен құқықтық реттелуі қысқаша қарастырылады. Ұлттық құқықтық актілерде және халықаралық құжаттарда қамтылған «киберқауіпсіздік» ұғымының анықтамалары талданды, жекелеген ғалымдар мен мамандардың осы ұғымды түсіндіруге көзқарастары зерттелді. Киберқауіпсіздікті қорғау объектілері әр түрлі елдердің киберқауіпсіздікті қамтамасыз ету туралы көзқарастарына сүйене отырып анықталды.

«Киберқауіпсіздік» және «ақпараттық қауіпсіздік» ұғымдарының функционалдық арақатынасына талдау жүргізілді, олардың арақатынасына көзқарас негізделген. Оның негізінде Ресей Федерациясында ақпараттық қауіпсіздікті қамтамасыз етудің қолданыстағы тәсілдері шеңберінде Киберқауіпсіздіктің мақсаттары мен міндеттерін шешу мүмкіндігі және елдегі киберқауіпсіздікті құқықтық реттеудің орынсыздығы туралы қорытынды жасалды.

Түйінді сөздер: ақпараттық қауіпсіздік; киберқауіпсіздік; ақпараттық-телекоммуникациялық желілер; ақпараттық технологиялар; ақпараттық инфрақұрылым; қорғау объектілері; Ресей Федерациясының ақпараттық қауіпсіздігі;

ақпарат пен ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету; ақпараттық инфрақұрылымның қауіпсіздігін қамтамасыз ету; деструктивті ақпараттық-психологиялық әсерден қауіпсіздікті қамтамасыз ету.

Annotation: The article briefly examines the status and legal regulation of the concept of "cyber security" in some foreign countries and in the Russian Federation. The definitions of the concept of "cyber security" contained in national legal acts and international documents are analyzed, the approaches of individual scientists and specialists to the interpretation of this concept are studied. The objects of cybersecurity protection based on the views of different countries on cybersecurity were determined.

An analysis of the functional relationship between the concepts of "cybersecurity" and "information security" was conducted, and an approach to their correlation was substantiated. On the basis of which the conclusion about the possibility of solving the goals and objectives of cybersecurity within the framework of existing approaches to ensuring information security in the Russian Federation and the inexpediency of legal regulation of cybersecurity in the country was made.

Keywords: information security; cybersecurity; information and telecommunications networks; information technology; information infrastructure; objects of protection; information security of the Russian Federation; ensuring the security of information and information resources; ensuring the security of information infrastructure; ensuring security against destructive information and psychological impact.

Информационно-телекоммуникационные сети (далее – ИТС) и информационные технологии (далее – ИТ), стремительно развитие которых мы наблюдаем в настоящее время, оказывают существенное влияние на все ключевые сферы деятельности граждан, организаций, общества и государства многих стран мира, в том числе и в Российской Федерации.

Внедрение и использование ИТС и ИТ в процессах управления как на государственном уровне, так и на уровне организаций и граждан является основой эффективного функционирования государственного аппарата и организаций, а также повышения качества жизни граждан.

В то же время вместе со значительным ростом возможностей ИТС и ИТ возникают риски возникновения новых и развития существующих угроз гражданам, организациям, обществу и государству в информационном пространстве или как чаще его сейчас называют виртуальным или киберпространством.

Как следствие существования киберпространства и использования его возможностей в целях обеспечения жизнедеятельности различных субъектов, неизбежно встает вопрос об обеспечении его безопасности. Примерно с начала века в ведущих западных странах начало формироваться новое направление национальной безопасности, связанное с киберпространством, которое получило название - кибербезопасность. С тех пор данное понятие достаточно широко используется как учеными и специалистами, так и обычными людьми.

Что же такое кибербезопасность, как оно сочетается с нормативными правовыми актами Российской Федерации, какое место

занимает в государственной системе информационной безопасности, как соотносится с другими направлениями информационной безопасности Российской Федерации?

Подобными вопросами задаются многие исследователи в области информационной безопасности в стране, высказываются различные мнения, порой диаметрально противоположные. В данной статье предпримем очередную попытку рассмотреть понятие «кибербезопасность», высказать авторскую, и поэтому, дискуссионную позицию по данному вопросу.

С целью анализа понятия «кибербезопасность» пойдем по нескольким направлениям: первое – анализ подходов к содержательному определению данного понятия в некоторых зарубежных странах и международных документах; второе – изучение мнений ученных и специалистов; третье – анализ правовых актов связанных степени с кибербезопасностью в стране.

Как было отмечено выше понятие «кибербезопасность» в развитых странах мира нашло свое применение еще с начала 21 века. В последствии и на международном уровне были разработаны документы международной безопасности, международные стандарты, декларации, обращения и другие документы, связанные с обеспечением кибербезопасности.

В настоящее время порядка сорока стран имеют национальные стратегии и иные документы в сфере кибербезопасности, в частности: Австралия, Великобритания, Израиль, Канада, Нидерланды, Норвегия, США, ЮАР, Япония и др. В этих странах данное понятие выделено в самостоятельную дефиницию. Особенно наглядно это видно на примере США [1; с. 8, 2; с. 63].

Так, комитет по системам национальной безопасности США (Committee on National Security Systems – CNSS) определил кибербезопасность как предотвращение повреждения, защита и восстановление компьютеров, систем и услуг электронной связи, включая содержащуюся в ней информацию для обеспечения её доступности, целостности и конфиденциальности, а также способность защищать и оборонять использование киберпространства от кибератак.

В документе CJCS «Cyberspace Operations» приводится определение безопасности киберпространства, а именно предпринимаемые в охраняемом киберпространстве действия для предупреждения несанкционированного доступа, эксплуатации или повреждения компьютеров, систем электронных коммуникаций и ИТ-систем, включая информационные технологии платформ, а также содержащейся в них информации для обеспечения её доступности, целостности, аутентификации, конфиденциальности и неотказуемости (non-repudiation).

Мы видим определение кибербезопасности через процесс, а объектами защиты являются информация, технические средства и коммуникации, а также программное обеспечение.

Национальная киберстратегия США, утвержденная в 2018 г., определяет в качестве своей цели повышение безопасности и устойчивости национальных и других информационных систем, критической инфраструктуры, информации, а также борьбу с киберпреступлениями [3; с.76].

Представляют интерес и подходы других государств, так, например, в Стратегии кибербезопасности эмирата Дубай под кибербезопасностью понимается – внедрение средств управления и контроля для защиты конфиденциальности, целостности и доступности данных для государственного и частного секторов Дубая и отдельных лиц. Мы видим, что в качестве объекта защиты рассматривается только информация.

Необходимо отметить, что регулирование правоотношений в киберпространстве, в том числе и регулирование вопросов обеспечения безопасности, исключительно на национальном уровне не обеспечит необходимого уровня безопасности в силу его трансграничности.

В стандарте ISO/IEC 27032:20121 «кибербезопасность» (или безопасность киберпространства) определяется как сохранение конфиденциальности, целостности и доступности информации в киберпространстве. Определение практически идентично определению «безопасности информации» приведенному в ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», а также созвучно положениям статьи 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4, 5].

То есть объектом защиты определена информация, которая обрабатывается в киберпространстве. Данное определение нельзя считать полным, так как из поля зрения полностью выпали такие компоненты как технические средства и программное обеспечение, являющиеся неотъемлемыми элементами киберпространства.

Международный союз электросвязи определяет «кибербезопасность» как набор инструментов, политик, концепций безопасности, руководств, подходов к управлению рисками, действий, обучения, лучших практик, гарантий и технологий, которые можно использовать для защиты киберсреды, а также активов организации и пользователей.

При этом активы организации и пользователей включают подключённые вычислительные устройства, персонал, инфраструктуру, приложения, услуги, телекоммуникационные системы и совокупность передаваемой и/или хранимой информации в киберсреде. Тут, в качестве объектов защиты, мы уже можем увидеть несколько элементов

– информацию, технические средства обработки информации, программное обеспечение и персонал.

В некоторых случаях «кибербезопасность» определяется через процесс, что не соответствует тем подходам, которые имеют место в российском законодательстве. Например, National Institute of Standards and Technology (NIST) определяет кибербезопасность как способность защищать и оборонять киберпространство от кибератак.

Как отмечено некоторыми авторами [6; с. 3, 3; с. 65], а также на основе анализа законодательных актов Российской Федерации, понятие «кибербезопасность» не нашло своего раскрытия в федеральном законодательстве Российской Федерации.

Тем не менее, утверждения о необходимости выделения в российском законодательстве, посвященному обеспечению информационной безопасности, направления «кибербезопасность» является предметом активного обсуждения в научной и законодательной среде.

В ноябре 2013 года в Совете Федерации Федерального Собрания Российской Федерации состоялись парламентские слушания, посвященные рассмотрению «Концепции стратегии кибербезопасности Российской Федерации». Ее авторы призывали создать национальную систему защиты от кибератак, усилить ответственность за киберпреступления и др. Однако в органах исполнительной власти данная инициатива не нашла поддержки на том основании, что проект концепции противоречит государственной политике страны в области информационной безопасности.

По сути, единственным правовым актом в Российской Федерации в котором дано определение понятия «кибербезопасность» является национальный стандарт Российской Федерации ГОСТ Р 56205-2014 (IEC/TS 62443-1-1:2009) «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели» [7]. Который определяет, что «кибербезопасность (киберзащита): Действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов».

Проводя даже поверхностный анализ данного определения, можно выявить некоторые нестыковки с российским законодательством, а именно:

1) мы видим отождествление понятий «безопасность» и «защита». В действующих законодательных и подзаконных актах Российской Федерации под безопасностью принято подразумевать состояние [8, 9, 10], а под защитой – процесс [4, 5];

2) не совсем понятно в каком смысле используются такие термины как «преобразование» и «рассекречивание». Первый из них не нашел своего отображения в законодательных и подзаконных актах связанных с информационной безопасностью, а второй – используется применительно только к вопросам защиты государственной тайны.

Конечно, мы не можем обойти стороной взгляды и подходы ученных и специалистов в данной сфере. В работах ряда авторов представлены интересные авторские определения [3; с.76, 2; с.66-68]. Проведя их изучение, мы можем сделать важные для нашей работы выводы:

1) как и ранее, в качестве объектов защиты выделяются информация и технические средства ее обработки;

2) наблюдается тесная связь между двумя понятиями «кибербезопасность» и «информационная безопасность», она отмечалась и при анализе других документов как национальных, так и международных. Однако мы не разделяем подходов автора, связанных с определением понятия «кибербезопасность» через понятие «информационная безопасность» [2; с.66-67] и уж тем более согласиться с мнением, что «…кибербезопасность представляет собой более широкое понятие, охватывающее, в том числе, информационную безопасность…» [3; с.78].

Свою позицию мы попробуем кратко обосновать ниже. А для этого необходимо определиться, а что такое «информационная безопасность» в контексте российского законодательства?

Правовой акт, который может дать нам ответ на поставленный вопрос, это Доктрина информационной безопасности Российской Федерации [10]. Проводя анализ определения исследуемого понятия, а также положений самой доктрины, считаем обоснованным высказать точку зрения о том, что информационная безопасность Российской Федерации включает в себя три направления:

1) обеспечение безопасности информации и информационных ресурсов;

2) обеспечение безопасности информационной инфраструктуры (вместе со связанным с ней программным обеспечением);

3) обеспечение безопасности от деструктивного информационного и информационно-психологического воздействия.

Определение «информационной безопасности» можно найти еще в порядке шести национальных стандартов Российской Федерации, однако в силу ограниченности объемов статьи, остановимся лишь на констатации того факта, что в этих стандартах объектами защиты устанавливаются либо информация, либо информация в совокупности с информационной инфраструктурой. С таким мнением мы также не можем согласиться.

По этой же причине выше мы говорили о несогласии определения «кибербезопасности» через понятие «информационная безопасность». Да, без условно, общий компонент у них есть, это – безопасность, но «безопасность», это не процесс, это состояние. Именно такой подход принят в российском законодательстве [8, 9].

Следующий аспект, это объекты защиты, то есть что является объектом защиты, когда мы говорим о кибербезопасности. В данном вопросе мы согласны с высказанными подходами некоторых национальных, международных документов, а также и специалистов, определивших в качестве объектов информацию и информационную инфраструктуру.

Так какое же место занимает кибербезопасность в системе информационной безопасности Российской Федерации?

Исходя из объектов кибербезопасности, можно сказать, что она включает в себя первые два направления информационной безопасности Российской Федерации, то есть обеспечение безопасности информации и информационной инфраструктуры без их разделения друг от друга и только в совокупности.

Тогда есть ли необходимость встраивания понятия «кибербезопасность» в систему информационной безопасности Российской Федерации? Вопрос крайне не простой и дискуссионный.

Автор статьи придерживается позиций, изложенных в существующих законодательных и иных правовых актах в данной области. Кроме этого, выражаем солидарность с мнением ряда ученых и специалистов, придерживающихся точки зрения о нестрогом и не устоявшимся характере понятия «кибербезопасность» [3; с.3, 2; с. 64], а в некоторых случаях можно говорить об использовании данного термина, по сути, как сленгового, например, в контексте понятия «киберпреступления».

Понятие «киберпреступления» не нашли своего юридического закрепления в уголовном законе Российской Федерации, поэтому использование данного термина применительно к преступлениям совершенным, с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации носит именно такой характер.

Таким образом, мы видим, что кибербезопасность является направлением информационной безопасности, причем нашедшим свое признание в зарубежных странах, преимущественно ведущих западных странах, особенно США. Также выражаем уверенность, что цели и задачи, стоящие перед кибербезопасностью вполне, можно решить на основе подходов, изложенных в Доктрине информационной безопасности Российской Федерации и федеральном законодательстве.

Не можем ни обратить внимание на положения Стратегии национальной безопасности Российской Федерации, утвержденной

Указом Президента Российской Федерации от 02.07.2021 № 400, в которой в качестве одного из стратегических национальных приоритетов Российской Федерации отмечена именно информационная безопасность.

Подводя итоги, хотелось бы отметить, что понятие «кибербезопасность» пришло из практики ведущих западных стран, где оно появилось и нашло свое применение в конце 90-х начале 2000-х годов. В последующем данное понятие нашло свое признание и в международной среде в части разработки некоторых международных стандартов, деклараций и других документов, прежде всего концептуального характера в области международной безопасности.

В Российской Федерации понятие «кибербезопасность» не нашло своего законодательного признания и если применяется, то только некоторыми негосударственными организациями.

С нашей точки зрения такая позиция государства вполне оправдана, прежде всего, в силу сложившегося подхода к вопросам обеспечения информационной безопасности, а также в силу неоднозначной трактовки данного понятия, как международными документами, так и ученными и специалистами. Кроме того, сущностная составляющая кибербезопасности нашла свою реализацию в других, более привычных для нас направлениях обеспечения информационной безопасности.

В этой связи можно констатировать тот факт, что дальнейшая юридическая «судьба» понятия «кибербезопасность» в России достаточно туманна, вызывая много вопросов и дискуссий.

Одно лишь ясно и не вызывает сомнений, это то, что цели и задачи, которые призвана решать кибербезопасность, являются важными и чрезвычайно актуальными.

Список использованной литературы:

1. Алексеев Г., Смирнов И. Противоборство в киберпространстве по взглядам военно-политического руководства ведущих зарубежных государств // Зарубежное военное обозрение №6, 2017. С.8-14.

2. Добродеев А.Ю. Кибербезопасность в Российской федерации. Модный термин или приоритетное технологическое направление обеспечения национальной и международной безопасности XXI века // Вопросы кибербезопасности №1(1), 2021. С.61-72.

3. Карцхия А. А. Новые элементы национальной безопасности: национальный и международный аспект // Вопросы кибербезопасности № 6(40), 2020. С. 72-81.

4. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». [Электронный ресурс] – Режим доступа: https://base.garant.ru/193664/ (дата обращения: 04.04.2023).

5. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». [Электронный ресурс] – Режим доступа:

https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 04.04.2023).

6. Марков А.С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности №1(47), 2022. С.2-9

7. ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009. Национальный стандарт Российской Федерации. «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели». [Электронный ресурс] – Режим доступа: https://base.garant.ru/71331784/ (дата обращения: 04.04.2023).

8. Федеральный закон Российской Федерации от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». [Электронный ресурс] – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 04.04.2023).

9. Федеральный закон Российской Федерации от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». [Электронный ресурс] – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 04.04.2023).

10. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». [Электронный ресурс] – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения: 04.04.2023).

УДК 004.01:355

Молдашева Айсулу Болатовна
Доцент кафедры военной истории и права Национального университета обороны имени Первого Президента Республики Казахстан – Елбасы Министерства обороны Республики Казахстан,
кандидат юридических наук
г. Астана, Республика Казахстан

Бергибаев Бахтияр Асылканович
Старший научный сотрудник – начальник научно-исследовательской лаборатории информационной безопасности Национального университета обороны имени Первого Президента Республики Казахстан – Елбасы Министерства обороны Республики Казахстан,
магистр
г. Астана, Республика Казахстан

НЕКОТОРЫЕ АСПЕКТЫ СТРАТЕГИИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. В статье исследованы вопросы цифровой трансформации, рассматриваются организационно-правовые основы цифровизации в воинской среде, в том числе с позиции систем обеспечения деятельности Вооруженных Сил Республики Казахстан. Изучены современные взгляды, правовая регламентация отдельных направлений цифровизации в сфере военного дела, возможность применения комплексно-правового подхода к построению системы цифровизации в Вооруженных Силах Республики Казахстан.

Автор уделяет внимание некоторым аспектам стратегии цифровой трансформации, базовому построению системы цифровизации с синхронизацией деятельности других систем обеспечения в области обороны и воинской службы.

В рамках статьи изучен опыт Соединенных Штатов Америки, Российской Федерации, который нашел свое отражение в руководящих документах стран. Исследованы возможные направления и способы применения искусственного интеллекта в военном деле. Практическая реализация исследованных вопросов рассматривается в контексте организационного обеспечения деятельности Вооруженных Сил Республики Казахстан, создания единого информационного пространства, баз данных в исследуемой области правоотношений, внедрение облачных сервисов, развитие собственного суверенного интернета, интеграция новых технологий в систему военного управления и межведомственной координации.

В работе, авторы в качестве методологической основы использует системный анализ и комплексно-правовой подход, которые позволяют исследовать вопросы цифровой трансформации в деятельности Вооруженных Сил Республики Казахстан и, в целом, служить основополагающим базисом построения системы цифровизации в воинской среде.

Отдельным блоком рассмотрены вопросы обеспечения кибербезопасности и возможность использования искусственного интеллекта в формировании информационно-коммуникационных систем по систематизации направлений деятельности органов военного управления.

Ключевые слова: стратегия; цифровая трансформация; воинская служба; военная безопасность; организационно-правовое обеспечение; искусственный интеллект; единая база данных; органы военного управления; информационно-коммуникационные технологии; организационно-техническая инфраструктура.

Аннотация. Мақалада цифрлық трансформация мәселелері зерттелді, әскери ортада, оның ішінде Қазақстан Республикасы Қарулы күштерінің қызметін қамтамасыз ету жүйелері тұрғысынан цифрландырудың ұйымдық-құқықтық негіздері қарастырылады. Қазіргі заманғы көзқарастар, әскери іс саласындағы цифрландырудың жекелеген бағыттарын құқықтық регламенттеу, Қазақстан Республикасының Қарулы Күштерінде цифрландыру жүйесін құруға кешенді-құқықтық тәсілді қолдану мүмкіндігі зерделенді. Авторлар цифрлық трансформация стратегиясының кейбір аспектілеріне, қорғаныс және әскери қызмет саласындағы басқа қамтамасыз ету жүйелерінің қызметін үндестіре отырып, цифрландыру жүйесінің негізгі құрылысына назар аударады. Мақала Америка Құрама Штаттарының, Ресей Федерациясының тәжірибесін зерттеді, ол осы елдердің басшылық құжаттарында көрініс тапты. Жасанды интеллектті әскери істе қолданудың мүмкін бағыттары мен тәсілдері зерттелді.

Зерттелген мәселелерді практикалық іске асыру Қазақстан Республикасы Қарулы күштерінің қызметін ұйымдастырушылық қамтамасыз ету, құқықтық қатынастардың зерттелетін саласында бірыңғай ақпараттық кеңістік, деректер базасын құру, бұлтты сервистерді енгізу, өзінің егеменді интернетін дамыту, әскери басқару жүйесіне жаңа технологияларды интеграциялау және ведомствоаралық үйлестіру контекстінде қаралады.

Жұмыста авторлар әдіснамалық негіз ретінде Қазақстан Республикасы Қарулы Күштерінің қызметіндегі цифрлық трансформация мәселелерін зерттеуге және тұтастай алғанда әскери ортада цифрландыру жүйесін құрудың іргелі негізіне қызмет етуге мүмкіндік беретін жүйелі талдау мен кешенді-құқықтық тәсілді пайдаланады.

Жеке блокта киберқауіпсіздікті қамтамасыз ету мәселелері және әскери басқару органдары қызметінің бағыттарын жүйелеу бойынша ақпараттық-коммуникациялық жүйелерді қалыптастыруда жасанды интеллектті пайдалану мүмкіндігі қарастырылған.

Түйінді сөздер: стратегия, цифрлық трансформация, әскери қызмет, әскери қауіпсіздік, ұйымдық-құқықтық қамтамасыз ету, жасанды интеллект, бірыңғай дерекқор, әскери басқару органдары, ақпараттық-коммуникациялық технологиялар, ұйымдық-техникалық инфрақұрылым.

Annotation. The article examines the issues of digital transformation, examines the organizational and legal foundations of digitalization in the military environment, including from the perspective of systems for ensuring the activities of the Armed Forces of the Republic of Kazakhstan. Modern views, legal regulation of certain areas of digitalization in the field of military affairs, the possibility of applying a comprehensive legal approach to the construction of a digitalization system in the Armed Forces of the Republic of Kazakhstan are studied.

The authors pay attention to some aspects of the digital transformation strategy, the basic construction of a digitalization system with synchronization of the activities of other support systems in the field of defense and military service. The article examines the experience of the United States of America, the Russian Federation, which is reflected in the governing documents of these countries. Possible directions and ways of using artificial intelligence in military affairs are investigated.

The practical implementation of the issues studied is considered in the context of organizational support for the activities of the Armed Forces of the Republic of

Kazakhstan, the creation of a unified information space, databases in the field of legal relations under study, the introduction of cloud services, the development of its own sovereign Internet, the integration of new technologies into the system of military management and interdepartmental coordination.

In the work, the authors use a systematic analysis and a comprehensive legal approach as a methodological basis, which make it possible to study the issues of digital transformation in the activities of the Armed Forces of the Republic of Kazakhstan and, in general, serve as a fundamental basis for building a digitalization system in the military environment.

In a separate block, the issues of ensuring cybersecurity and the possibility of using artificial intelligence in the formation of information and communication systems to systematize the activities of military authorities are considered.

Keywords: strategy, digital transformation, military service, military security, organizational and legal support, artificial intelligence, unified database, military authorities, information and communication technologies, organizational and technical infrastructure.

Введение. Военная безопасность важнейшая составляющая безопасности государства. В деле обеспечения военной безопасности и защиты Республики Казахстан – построение системы информационно-технологического обеспечения, формирование единого информационного пространства в военной среде, защита и обеспечение кибербезопасности являются приоритетными направлениями дальнейшего развития Вооруженных Сил Республики Казахстан.

Основная часть. Как известно, постановлением Правительства Республики Казахстан от 28 марта 2023 года утверждена Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 - 2029 годы.

Содержательная часть документа определяет, что «внедрение платформенной модели позволит построить эффективный государственный аппарат, направленный на решение жизненных ситуаций граждан наиболее удобным путем, а также максимизация и агрегация актуальных онлайн данных для возможности применения инструментов искусственного интеллекта при моделировании сценариев и принятия решений".

Будет создана национальная система искусственного интеллекта на базе Smart Data Ukimet, которая позволит прогнозировать и принимать решения на основе достоверных данных.

В перспективе по результатам реализации документа будет создана Единая платформа "электронного правительства", предусматривающая сквозную межведомственную цифровизацию процессов и создание комплексной организационно-технической инфраструктуры как для предоставления услуг, так и для обеспечения деятельности системы государственного управления» [1].

В данном контексте, поиск новых путей дальнейшего развития и совершенствования блока информационно-технологического обеспечения является актуальной темой для современной Армии.

Общим устремлением, объединяющим все концепции в деле цифровой трансформации, является их ориентация на идею укрепления цифрового пространства, грамотности, научного, методического, правового сопровождения данного процесса.

Создание информационно-технологической основы в воинской среде на современном этапе является приоритетным направлением.

Так, «одной из важнейших технологий, применяемой для повышения потенциала ВС, становится искусственный интеллект. В стратегии национальной обороны» США составной частью, которой является «Стратегия искусственного интеллекта отмечается, что искусственный интеллект «изменит общество и в итоге характер войны [2,С.113].

«Использование искусственного интеллекта в системах управления необходимо для повышения общей ситуационной осведомленности и распознавания возникающих опасностей. Путем сбора и обработки всей доступной информации, полученной от различных источников, возможно формирование интегрированного источника информации, так называемой «глобальной оперативной картины», на основе которой командирам различного уровня будут предлагаться наиболее эффективные варианты действий» [2, С.114].

Основное внимание в вопросах приоритетных направлений Стратегии цифровой трансформации уделено организации и проведению работы в поддержании должного уровня боевой готовности, защиты и обеспечения кибербезопасности, повышения уровня цифровой грамотности личного состава в рамках реализации общенациональной, государственной политики в области цифровизации.

Функционирование данной системы позволит внедрить облачные сервисы для прозрачности расходов и мониторинга безопасности, развить собственный суверенный интернет и внедрить другие технологии. В свою очередь, интеграция новых технологий в систему военного управления и межведомственной координации, создание условий и действенных механизмов позволит достичь высокой степени ее функциональности и решать задачи в области обеспечения военной безопасности.

Необходимость научного, методического и правового сопровождения развития цифровизации и совершенствования работы в данном направлении очевидна.

Стратегия цифровой трансформации в Вооруженных Силах Республики Казахстан определяет следующие задачи:

- формирование единого цифрового пространства для воинских частей и учреждений;

- разработка целостной системы по учету вооружения, военной техники и материальных средств (это позволит упразднить административные процессы по ведению бумажных документов на 80%, высвободив тем самым временные ресурсы для выполнения мероприятий);

- внедрение цифровых систем, позволяющих решить проблемы с суицидальными проявлениями путем, оснащения воинских частей видеокамерами, цифровыми браслетами, которые будут показывать местонахождение служащего и измерять его пульс.

Положительной тенденцией в исследуемой области отмечается реализация Министерством обороны Республики Казахстан в рассматриваемой области проекта «Цифровые офицеры». Впервые в органах военного управления проходят службу "цифровые офицеры", которые являются связующим звеном в вопросах внедрения в жизнедеятельность вооруженных сил процессов информационных технологий, инноваций и выступать инициаторами единой политики цифрового развития Вооруженных Сил Республики Казахстан.

По мнению военных специалистов, реализация проекта «Цифровизация для призывников» позволит минимизировать коррупционные риски. Проект предусматривает возможность лицам, призывного возраста при наличии оснований, получить отсрочку от армии через портал электронного правительства. Перевод в электронный формат позволит на постоянной основе актуализировать информацию о прохождении призывником медицинских комиссий в лечебных заведениях по месту прописки, исключить понятие приписной карты из обращения, военный билет будет иметь цифровой формат.

Это коснется и студентов, которые смогут получить услугу отсрочки и освобождения от призыва в проактивном режиме. При наличии инвалидности граждане автоматически будут освобождены от службы в армии. Отпадает также необходимость постановки и снятия с воинского учета военнообязанных и призывников в случае миграции.

Несомненно, решать задачи формирования и развития цифровизации армии, возможно благодаря устойчивому функционированию информационно-технологической системы, организационно-технической инфраструктуры государства и соответствующей правовой основы.

При этом, концептуальность цифровизации систем обеспечения должна заключатся в применении комплексно-правового подхода, изучения системы взглядов, основная составляющая которых базируется на научном обосновании ее методов, прикладных основ. Несомненно, эта система требует постоянного совершенствования и развития.

К примеру, «в Китае в настоящее время принят и используется ряд законодательных актов, регламентирующих стратегию страны в киберпространстве. Закон о кибербезопасности вступил в юридическую силу с 1 июня 2017 года. Закон о кибербезопасности регламентирует действия серверов и услуг по сбору, хранению и обработке пользовательских данных, определяет порядок и специфику обеспечения безопасности информационной инфраструктуры в стратегически важных отраслях. Главной целью принятия закона провозглашается защита национального «киберсуверенитета» КНР» [3, С.18]. Кроме того, действует Национальная стратегия безопасности в киберпространстве КНР. «В этом документе китайская сторона впервые изложила свою позицию и понимание кибербезопасности, перспективы преобразования системы государственного управления сетевым пространством и возможности построения единого интернет-сообщества» [3, С.19].

На наш взгляд, основными подходами и принципами построения стратегии цифровой трансформации должны выступать:

- научный подход и конкретность, опора на современные знания, методики и технологии;
- профессиональный подход;
- своевременность, целесообразность принятия решений, прогнозирование их социальных, правовых и других последствий;
- целенаправленность, реальность и рациональность действий;
- единство всех составляющих направлений развития цифровизации.

Выводы. Комплексно-правовой подход к построению системы цифровизации в воинской среде должен представлять собой систему организационно-правовых основ, системных мер при организации, прежде всего, работы области систем обеспечения деятельности Вооруженных Сил Республики Казахстан.

В данном контексте, стратегия цифровой трансформации служит плацдармом для развития и построения информационно-технологической основы в деле обеспечения кибербезопасности. Реализация стратегии цифровой трансформации будет способствовать интеллектуализации казахстанской армии и повышению ее боеготовности и боеспособности.

Список использованных источников:

1. Утверждена концепция цифровой трансформации и развития отрасли технологий до 2029 года. [Электронный ресурс] – Режим доступа https://www.zakon.kz/6391650-utverzhdena-kontseptsiya-tsifrovoy-transformatsii-i-razvitiya-otrasli-tekhnologiy-do-2029-goda (дата обращения: 26.04.2023).

2. Галкин Д., Коляндра П., Степанов А. Состояние и перспективы использования искусственного интеллекта в военном деле // Военно-теоретический журнал «Военная мысль» №1 - Москва. 2021. С.157.

3. Носов С. Система кибербезопасности Китая //Зарубежное военное обозрение №2- Москва, 2021 г.С.111.

УДК 004.056.53

Севрюк Дмитрий Валерьевич
Аспирант ФГНИУ «Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации»,
г. Москва, Российская Федерация

КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВА ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА

Аннотация. В условиях сформировавшегося информационного общества – общества информационных сетей и технологий, – существенным элементом обеспечения независимой политики государства необходимо признать обеспечение компьютерной безопасности. Возрастающий рост информационных угроз приводит к тому, что незаконные вторжения в киберпространстве выходят из разряда преступлений против отдельного гражданина и перерастают в угрозу безопасности государства, в связи с чем необходимость обеспечения кибербезопасности становится еще более актуальной. В статье рассматривается роль кибербезопасности в обеспечении государственного суверенитета, а также описываются существующие угрозы и вызовы в области кибербезопасности и основные меры, которые могут быть приняты для защиты государственных интересов.

Ключевые слова: кибербезопасность; государственный суверенитет; информационные угрозы; критическая информационная инфраструктура; международное сотрудничество.

Аннотация. Қалыптасқан ақпараттық қоғам – ақпараттық желілер мен технологиялар қоғамы жағдайында мемлекеттің тәуелсіз саясатын қамтамасыз етудің маңызды элементі ретінде компьютерлік қауіпсіздікті қамтамасыз етуді тану қажет. Ақпараттық қауіптердің артуы киберкеңістіктегі заңсыз басып кірулердің жекелеген азаматқа қарсы қылмыстар санатынан шығып, мемлекеттің қауіпсіздігіне қатерге ұласуына алып келеді, осыған байланысты киберқауіпсіздікті қамтамасыз ету қажеттілігі одан да өзекті бола түсуде. Мақалада мемлекеттік егемендікті қамтамасыз етудегі киберқауіпсіздіктің рөлі қарастырылады, сонымен қатар киберқауіпсіздік саласындағы қауіптер мен қиындықтар және мемлекеттік мүдделерді қорғау үшін қабылдануы мүмкін негізгі шаралар сипатталған.

Түйінді сөздер: киберқауіпсіздік; мемлекеттік егемендік; ақпараттық қауіптер; маңызды ақпараттық инфрақұрылым; халықаралық ынтымақтастық.

Annotation: In the context of the emerging information society – a society of information networks and technologies - ensuring computer security is an essential element of a state's independent policy. The increasing growth of information threats leads to the fact that illegal intrusions into cyberspace go beyond crimes against individual citizens and become a threat to national security, making the need to ensure cybersecurity even more relevant. The article discusses the role of cybersecurity in ensuring state sovereignty, as well as describes existing threats and challenges in the field of cybersecurity and the main measures that can be taken to protect national interests.

Keywords: cybersecurity; state sovereignty; information threats; critical information infrastructure; international cooperation.

Современное общество, как в рамках отдельного государства, так и в рамках международного сообщества все больше зависит от цифровых технологий и аппаратного комплекса с ним связанного. Новейшие технологии проникают если не во все, то в большинство наиболее важных сфер жизни: от банковской системы и государственного управления до бытовых устройств и устройств персонального использования. Вместе с тем стало очевидным, что использование цифровых технологий сопряжено с существенными рисками, связанными с кибербезопасностью. Кибербезопасность в свою очередь является важной составляющей государственного суверенитета.

Под суверенитетом государства традиционно понимается его право и способность принимать независимые решения по управлению внутренними политическими процессами и обеспечению внешней политики вне контекста оказываемого влияния. Однако в условиях, когда цифровая среда проникла в ключевые сферы государственного управления, нарушения кибербезопасности могут повлиять на способность государства реализовывать свой суверенитет.

На текущий момент различные информационные системы составляют ядро государственного и частного корпоративного управления, являются неотъемлемой частью механизма государства [1]. Указанные системы обеспечивают хранение, обработку, передачу и анализ большого объема информации, необходимой для принятия решений и управления различными процессами.

В государственном управлении информационные системы играют важную роль, обеспечивая эффективность и прозрачность работы органов власти. Они используются для учета и обработки информации о гражданах, бизнесе, налогах, социальной защите, здравоохранении, образовании, безопасности и других сферах. Такие системы также могут использоваться для контроля за исполнением законов и управления экономическими процессами в целом.

Таким образом, информационные системы являются неотъемлемой частью современной экономики и общества, обеспечивая эффективность и прозрачность управления, повышение качества продукции и услуг, а также улучшение жизни людей. В будущем, с развитием технологий, информационные системы будут играть еще более важную роль, становясь основой цифровой экономики и общества. Именно по причине распространенности и обширности информационных систем обеспечение их неуязвимости есть ключевая задача для современного государства.

В условиях деглобализации и обострения противоречий существенную роль играет тенденция к суверенизации информационного пространства, ранее предполагаемого в качестве глобального [2]. Однако пропорционально вырастает количество угроз

кибербезопасности государств. Так, пресс-службой Министерства внутренних дел Российской Федерации отмечалось, что за 2022 год каждое четвертое преступление совершено с использованием информационных технологий, в частности 92,2 % заведомо ложных сообщений об актах терроризма совершены дистанционно [3]. Крупнейшие кибератаки уже минимум два десятилетия наносят вред реализации суверенных полномочий отдельных государств, например атака компьютерными вирусами Stuxnet и Flame иранской ядерной программы в 2010 – 2012 годах привела к существенному снижению функционирования атомных электростанций, что повлекло за собой последствия для энергетической системы Ирана [4].

Защите суверенитета Российской Федерации в информационном пространстве уделено большое внимание в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646 [2; с.5], [5]. Кибербезопасность в таких условиях есть необходимый элемент национальной безопасности.

Под кибербезопасностью можно понимать состояние сохранности, функциональной устойчивости национального информационного поля, неуязвимости информационной и телекоммуникационной инфраструктуры, защищенность критически важных объектов и недоступность информации, способной оказывать влияние на принятие государственными органами решений по реализации политической власти. Таким образом, кибербезопасность охватывает широкий спектр мер по защите информации и инфраструктуры от киберугроз. Киберугрозы могут быть связаны с киберпреступностью, кибершпионажем, кибертерроризмом и другими формами киберактивности.

Представляется, что обеспечение такого состояния может быть возможным только в случае последовательной государственной политики, направленной на модернизацию и суверенизацию аппаратно-программного обеспечения, систем обработки, хранения и передачи данных, что потребует существенного внимания государства к имеющимся разработкам в области информационной инфраструктуры Российской Федерации и формирование собственного вектора развития информационно-телекоммуникационных технологий, аппаратного комплекса и систем своевременного обнаружения и пресечения возникающих киберугроз.

Кроме того, необходимо выделить следующие направления деятельности государства, которые позволят обеспечить кибербезопасность:

1) Создание региональных и межрегиональных центров компьютерной безопасности, призванных выявлять и отражать кибератаки на информационную инфраструктуру;

2) Переход на отечественное программное обеспечение, разрабатываемое для отечественных микропроцессорных архитектур, его регулярное обновление и совершенствование;

3) Информационное просвещение сотрудников государственного аппарата и всего населения, в том числе информирование о состоянии актуальных угроз кибербезопасности, основных принципах «компьютерной гигиены»;

4) Формирование системы аудита безопасности: осуществление регулярных модельных атак на ключевые объекты информационной инфраструктуры с отработкой механизмов отражения и подавления;

5) Сегментация информационных баз данных в целях возможной оперативной изоляции пораженных участков;

6) Развитие международного сотрудничества в области противодействия киберугрозам, в первую очередь со странами-участниками ЕАЭС, БРИКС, ШОС.

Таким образом, на сегодняшний день кибербезопасность является важной составляющей суверенитета современного государства. В условиях зависимости государств от цифровых технологий и угроз, связанных с использованием этих технологий, обеспечение высокого уровня кибербезопасности становится необходимостью. Развитие соответствующей инфраструктуры, создание специализированных учреждений, совершенствование законодательства и международное сотрудничество позволят обеспечить проведение независимой политики, гарантировать устойчивость общества в контексте усиливающихся киберугроз. Именно государству отведена особая роль в формировании безопасности национального информационного пространства вследствие чего, именно от него потребуются воля и решимость, а также ресурсы для ее обеспечения.

Список использованных источников:

1. Голубкина К.В., Абрамян С.К. Электронное правительство и электронная демократия как новые явления информационного общества // Гуманитарные, социально-экономические и общественные науки. 2018. №1. [Электронный ресурс] - Режим доступа: https://cyberleninka.ru/article/n/elektronnoe-pravitelstvo-i-elektronnaya-demokratiya-kak-novye-yavleniya-informatsionnogo-obschestva (дата обращения: 24.04.2023).

2. Ефремов А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации [Текст]: дис. ... докт. юрид. наук: 12.00.13: защищена 21.04.2021: утв. 21.04.2021 / Ефремов Алексей Александрович. - М., 2020. - 418 с.

3. См. Статистические сведения о состоянии преступности в 2022 году. [Электронный ресурс] - Режим доступа: https://mvdmedia.ru/news/official/statisticheskie-svedeniya-o-sostoyanii-prestupnosti-v-2022-godu (дата обращения: 24.04.2023).

4. См. "Лаборатория Касперского" нашла "самый сложный" вирус. [Электронный ресурс] - Режим доступа: https://lenta.ru/news/2012/05/28/flame/ (дата обращения: 27.04.2023).

5. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – 2016 - №50. – Ст.7074. / [Электронный ресурс]: СПС Консультант Плюс – 2023 – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_208191 / (дата обращения 22.04.2023).

УДК 004.8:341.231.14

Сейтаева Жанар Секежановна
Заведующий кафедрой специальной подготовки по противодействию глобальным угрозам Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан
кандидат юридических наук, ассоциированный профессор,
старший советник юстиции
г. Астана, Республика Казахстан

СОБЛЮДЕНИЕ ПРАВ ЧЕЛОВЕКА ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Аннотация. В настоящей публикации исследуются этические дилеммы и вызовы, связанные с использованием искусственного интеллекта в правоохранительной деятельности в контексте соблюдения основных прав человека.

В статье освещаются отдельные факторы негативного влияния систем ИИ на соблюдение основных прав человека, возможные риски по усилению предвзятости и дискриминации в отношении определенных групп людей, а также потенциальные нарушения неприкосновенности частной жизни и защиты персональных данных.

Автором предлагается несколько вариантов решения этих этических проблем, таких как разработка этических руководящих принципов и кодексов поведения для разработчиков и пользователей искусственного интеллекта, повышение прозрачности и подотчетности при принятии решений с использованием искусственного интеллекта и инвестирование в исследования и разработки систем искусственного интеллекта, в которых приоритетным является соблюдение прав человека.

В заключение в статье делается вывод о том, что, хотя существуют значительные проблемы с обеспечением уважения прав человека в контексте искусственного интеллекта, существуют также возможности для инноваций и прогресса в этой области, которые могут принести пользу обществу в целом.

Ключевые слова: права человека; искусственный интеллект; системы искусственного интеллекта; неприкосновенность частной жизни; правоохранительная деятельность.

Аннотация. Бұл басылым адамның негізгі құқықтарын сақтау контекстінде құқық қорғау қызметінде жасанды интеллектті қолдануға байланысты этикалық дилеммалар мен қиындықтарды зерттейді.

Мақалада жасанды интеллект жүйелерінің адамның негізгі құқықтарының сақталуына теріс әсерінің жекелеген факторлары, адамдардың белгілі бір топтарына қатысты біржақтылық пен кемсітушілікті күшейту бойынша ықтимал тәуекелдер, сондай-ақ жеке өмірге қол сұғылмаушылық пен дербес деректерді қорғаудың ықтимал бұзылулары баяндалады.

Автор осы этикалық мәселелерді шешудің бірнеше нұсқаларын ұсынады, мысалы, жасанды интеллектті жасаушылар мен пайдаланушылар үшін этикалық нұсқаулар мен мінез-құлық кодекстерін әзірлеу, жасанды интеллектті қолдана отырып шешім қабылдауда ашықтық пен есеп беруді арттыру және адам құқықтарын сақтау басым болатын жасанды интеллект жүйелерін зерттеу мен әзірлеуге инвестициялау.

Қорытындылай келе, мақалада жасанды интеллект контекстінде адам құқықтарын құрметтеуге қатысты маңызды мәселелер болғанымен, жалпы қоғамға пайда әкелетін осы саладағы инновациялар мен прогреске мүмкіндіктер бар деген қорытындыға келеді.
Түйінді сөздер: адам құқықтары; жасанды интеллект; жасанды интеллект жүйелері; жеке өмірге қол сұғылмаушылық; құқық қорғау қызметі.

Annotation. This publication examines the ethical dilemmas and challenges associated with the use of artificial intelligence in law enforcement in the context of respect for fundamental human rights.

The article highlights certain factors of the negative impact of AI systems on the observance of fundamental human rights, possible risks of increasing bias and discrimination against certain groups of people, as well as potential violations of privacy and personal data protection.

The author suggests several solutions to these ethical problems, such as the development of ethical guidelines and codes of conduct for developers and users of artificial intelligence, increasing transparency and accountability in decision-making using artificial intelligence, and investing in research and development of artificial intelligence systems in which respect for human rights is a priority.

In conclusion, the article concludes that although there are significant challenges in ensuring respect for human rights in the context of artificial intelligence, there are also opportunities for innovation and progress in this area that can benefit society as a whole.
Keywords: human rights; artificial intelligence; artificial intelligence systems; privacy; law enforcement.

За последние десятилетия актуальным становится обсуждение вопросов использования искусственного интеллекта (ИИ) в ряде контекстов правоохранительной и судебной деятельности, включая предупреждение преступности, уголовное преследование и судебное рассмотрение.

Исследователями отмечается, что искусственный интеллект может быть применим:

- для анализа данных и выявления закономерностей, которые могут указывать на вероятность совершения преступлений. Используя ИИ в прогностических целях, правоохранительные органы могут более эффективно распределять ресурсы и разрабатывать целевые стратегии предупреждения преступности. Обработка естественного анализа больших объемов текстовых данных, таких как сообщения в социальных сетях, электронные письма и расшифровки чатов, также могут помочь в выявлении потенциальных угроз или преступной деятельности;

- в системах распознавания лиц для идентификации подозреваемых и пропавших без вести. Органы правопорядка могут использовать эти системы для сканирования видеозаписей с камер наблюдения и сопоставления лиц с криминальным прошлым;

- для анализа доказательств. ИИ можно использовать для ускоренного и точного анализа судебно-медицинских доказательств, таких как образцы ДНК, отпечатки пальцев и баллистические доказательства;

- при управлении дорожным движением: для анализа данных и помощи полиции в управлении транспортным потоком и повышении безопасности на дорогах [1].

В то же время, необходимо отметить, что существуют также и опасения по поводу возможного неправомерного использования ИИ в правоохранительной деятельности, в том числе приводящего к нарушению основных прав человека.

В 2015 году Организация Объединенных Наций открыла в Гааге Центр ИИ и робототехники, после чего созвала международную конференцию для обмена мнениями по будущей стратегии в этой области [2].

Уже два года спустя учеными-правоведами начинается изучение связи между новыми технологиями и соблюдением прав человека. Так, Х.Лю и К.Завеска, отмечая, неоднозначную роль ИИ при соблюдении основных прав человека, выступили за новый их набор, способный работать с робототехникой и машинами.

С этого момента влияние ИИ на права человека критически анализируется учеными с различных позиций: с точки зрения трудовых отношений, моделей рабочего времени и вознаграждения, которые, как ожидается, претерпят серьезные изменения из-за более широкого использования ИИ; с ракурса использования дискриминационных алгоритмов, затрагивающих почти все права, содержащиеся во Всеобщей декларации прав человека и т.п.

В 2019 году, Европейский Союз после разработки своей стратегии в отношении ИИ, опубликовал свой первый скоординированный план действий по продвижению надежного ИИ с помощью этических норм и политики. При этом государствам-участникам Европейского Союза предлагались следующие этические ориентиры:

- разработка и использование систем ИИ в соответствии с уважением автономии человека, справедливостью и предотвращением любых нарушений;

- уделением особого внимания ситуациям, касающимся таких уязвимых групп, как дети, люди с ограниченными возможностями и другие группы, исторически находящиеся в неблагоприятном положении или подверженные риску изоляции, а также ситуациям, характеризующимся асимметрией власти или информации, например, между работодателями и работниками;

- принятием надлежащих мер для снижения рисков негативных последствий воздействия ИИ на демократию и верховенство закона [4].

В Республике Казахстан рассмотрение вопросов порядка использования ИИ, определение его статуса и правовых последствий заложено в Плане действий по реализации Концепции правовой политики Республики Казахстан до 2030 года, утвержденном постановлением Правительства РК от 29 апреля 2022 года № 264.

Этим же постановлением предусматривается внесение предложений в Администрацию Президента РК касательно кодификации норм права, регулирующих важнейшие общественные отношения в сфере информационно-коммуникационных технологий, связи, обработки данных, цифровых активов, автоматизации промышленности, информационной безопасности, машинного обучения и ИИ, защиты прав субъектов персональных данных [5].

Считаем разрешение указанных вопросов чрезвычайно важными, в связи с возможностью возникновения целого ряда рисков использования ИИ в правоохранительной деятельности.

Например, есть опасения по поводу возможной систематической ошибки и дискриминации в алгоритмах ИИ, особенно если данные, используемые для обучения этих алгоритмов, необъективны. Есть также опасения по поводу того, что ИИ может нарушать права на неприкосновенность частной жизни, особенно если он используется для отслеживания перемещений или действий людей.

Попытаемся выделить отдельные факторы негативного влияния систем ИИ на соблюдение основных прав человека.

Предвзятость и дискриминация. Системы ИИ могут усилить предубеждения и дискриминацию в отношении определенных групп людей, особенно из маргинализированных сообществ. При этом, алгоритмы ИИ могут усилить существующее неравенство и дискриминационные практики.

Приведем несколько примеров:

Системы ИИ учатся на основе данных и если данные, используемые для их обучения, являются неполными, система ИИ может принимать предвзятые решения. Например, если алгоритм распознавания лиц обучен на наборе данных, состоящем преимущественно из белых лиц, он может быть не столь точным, когда дело доходит до распознавания лиц людей с более темными тонами кожи, что приводит к дискриминационным результатам.

Системы ИИ также могут усиливать существующие человеческие предубеждения. Например, если система ИИ обучена на данных, отражающих общественные предрассудки, она может научиться дискриминировать определенные группы людей. Это может произойти при принятии решений о найме или предоставлении кредита, когда система ИИ может дискриминировать кандидатов на основе таких факторов, как раса, пол или религия.

Еще одним фактором, который может способствовать дискриминации системами ИИ, является отсутствие разнообразия в командах, разрабатывающих их. Если все люди, разрабатывающие алгоритмы, имеют схожее образование или схожий опыт, они могут быть не в состоянии распознать предубеждения в системе.

Системы ИИ также могут усиливать стереотипы об определенных группах людей. Например, если чат-бот запрограммирован на взаимодействие с клиентами определенным образом, это может усилить стереотипы о том, как следует относиться к женщинам или людям не титульной нации.

Конфиденциальность и защита данных. Для эффективного функционирования системам ИИ часто требуется доступ к большим объемам персональных данных. Сбор, обработка и хранение персональных данных системами ИИ могут создавать риски для конфиденциальности и защиты данных.

Примерами нарушения конфиденциальности и защиты данных людей можно назвать следующее:

Утечка данных. В случае, когда система ИИ не предназначена для защиты данных и предотвращения их утечек, это может привести к раскрытию конфиденциальной личной информации, такой как финансовая информация, медицинские записи и личная идентификационная информация.

Также, системы ИИ могут использоваться для мониторинга поведения и деятельности людей, включая их онлайн-активность, физические перемещения и социальные взаимодействия, что может быть нарушением прав на неприкосновенность частной жизни.

Кроме того, системы ИИ также могут нарушать права на неприкосновенность частной жизни, увековечивая алгоритмическую предвзятость, которая представляет собой несправедливое или дискриминационное отношение к определенным группам людей на основе их расы, пола, этнической принадлежности или других личных характеристик. Это может привести к исключению определенных групп из определенных возможностей или к чрезмерной представленности определенных групп в определенных контекстах.

И наконец, системы ИИ могут быть разработаны для сбора и анализа больших объемов данных о людях, которые могут быть использованы для создания подробных профилей поведения, предпочтений и привычек людей. Это может привести к агрессивной и необоснованной слежке за отдельными лицами, а также может быть использовано для принятия решений, влияющих на их жизнь, таких как определение их кредитоспособности или права на получение определенных услуг.

Подотчетность и прозрачность. Важное значение для защиты прав человека имеет обеспечение прозрачности того, как системы ИИ разрабатываются, внедряются и используются. Поскольку системы ИИ могут быть сложными для понимания, это может затруднить определение ответственности, когда что-то пойдет не так. В этой связи необходимы четкие рекомендации и стандарты для систем ИИ, что поможет обеспечить прозрачность и подотчетность их использования.

Кроме перечисленных факторов, необходимо отметить также влияние систем ИИ на соблюдение таких прав и свобод человека, как труд и человеческое достоинство (системы искусственного интеллекта все чаще используются для автоматизации рабочих мест и выполнения задач, которые ранее выполнялись людьми. Это может представлять угрозу человеческому достоинству и благополучию, особенно если работники увольняются или их труд обесценивается); свобода слова и информации (системы искусственного интеллекта могут использоваться для фильтрации или цензуры информации, потенциально нарушая свободу выражения мнений и информации); доступ к правосудию и справедливости.

Таким образом, на сегодняшний день необходимо констатировать двоякое влияние ИИ на права человека: с одной стороны, определяются большие возможности в предупреждении преступности, уголовном преследовании и судебном рассмотрении, с другой стороны, четко обозначены угрозы нарушения отдельных прав человека.

При всей полезности ИИ, важно учитывать потенциальные риски и этические последствия, а также обеспечивать его использование таким образом, чтобы уважать права и свободы личности. Таким образом можно использовать преимущества этой прогрессивной технологии, сводя к минимуму ее потенциальный вред.

В этих целях, предлагаем несколько возможных вариантов решения этических проблем, связанных с использованием ИИ в области соблюдения основных прав человека:

- разработка и установление этических стандартов и руководящих принципов, предписывающих надлежащее использование ИИ с соблюдением основных прав человека;
- создание нормативно-правовой базы, устанавливающей рамки использования ИИ, особенно в таких областях, как неприкосновенность частной жизни, недискриминация и прозрачность;
- способствование сотрудничеству между разработчиками ИИ и экспертами по правам человека, для выявления потенциальных предубеждений, дискриминационных результатов и других этических проблем в их технологиях;
- повышение прозрачности в отношении данных и алгоритмов, используемых в системах ИИ;
- расширение возможности граждан по контролю над своими личными данными и предоставление им информации о том, как используются эти данные;
- проведение регулярных аудитов систем ИИ независимыми сторонними организациями, чтобы гарантировать, что они разработаны и используются таким образом, чтобы соблюдались основные права человека;

- обеспечение образования и профессиональной подготовки сотрудников компаний, использующих ИИ, по вопросам их этичного использования.

Список использованных источников:

1. Кобленков А.Ю. «О перспективах использования цифровизации и искусственного интеллекта в качестве технологий обеспечения личной безопасности граждан и сотрудников полиции // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2022. No 1 (57). С. 147—152 // [Электронный ресурс] – Режим доступа: https://doi.org/10.36511/2078-5356-2022-1-147-152; Барчуков В.К. «Систематизация и совершенствование правового регулирования применения искусственного интеллекта в правоохранительной деятельности» // Российский журнал правовых исследований. Том 7, № 1 (2020). С. 106-112 // [Электронный ресурс] – Режим доступа: https://journals.eco-vector.com/2410-7522/article/view/34958; Суходолов А. П. Искусственный интеллект в противодействии преступности, ее прогнозирование, предупреждение и развитие / А. П. Суходолов, А. М. Бычкова // Всероссийский криминологический журнал. — 2018. — Т. 12, № 6. — С. 753–766 // [Электронный ресурс] – Режим доступа: http://cj.bgu.ru/reader/article.aspx?id=22308; Jesus Mena «Machine Learning Forensics for Law Enforcement, Security, and Intelligence», 2011 // [Электронный ресурс] – Режим доступа: https://www.taylorfrancis.com/books/mono/10.1201/b11026/machine-learning-forensics-law-enforcement-security-intelligence-jesus-mena (дата обращения 10.04.2023 г.)

2. Nations Unies. Union Internationale de Telecommunications. United Nations Activities on Artificial Intelligence. Geneva: ITU Publications; 2018. Available from: https://www.itu.int/pub/S-GEN-UNACT-2018-1;

3. Liu HY, Zawieska K. From responsible robotics towards a human rights Regime oriented to the challenges of robotics and artificial intelligence. *Ethic Inf Technol*. 2017; 22:1–13 // [Электронный ресурс] – Режим доступа: https://link.springer.com/article/10.1007/s10676-017-9443-3 (дата обращения 10.04.2023 г.)

4. A European approach to artificial intelligence // [Электронный ресурс] – Режим доступа: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (дата обращения 10.04.2023 г.)

5. Постановление Правительства Республики Казахстан от 29 апреля 2022 года № 264 «Об утверждении Плана действий по реализации Концепции правовой политики Республики Казахстан до 2030 года» // [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/P2200000264#z2 (дата обращения 10.04.2023 г.)

УДК 004.056.52:34

Чуешов Кирилл Викторович
Заместитель начальника отдела проблем укрепления законности в сфере экономической деятельности государственного учреждения «Научно-практический центр проблем укрепления законности и правопорядка Генеральной прокуратуры Республики Беларусь, г. Минск, Республика Беларусь

ПРАВОВЫЕ ОСНОВЫ ФОРМИРОВАНИЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Аннотация. В статье на основе анализа положений нормативных правовых актов, регулирующих вопросы информационной безопасности и кибербезопасности в Республике Беларусь, рассматриваются предпосылки формирования и особенности национальной системы обеспечения кибербезопасности, задачи и функции государственных органов и организаций, определяются направления дальнейшего совершенствования подходов правового регулирования данной сферы общественных отношений.
Ключевые слова: информационная безопасность; кибербезопасность; национальная система обеспечения кибербезопасности; информационная инфраструктура; кибератака; киберинцидент; кибертерроризм, киберустойчивость.

Аннотация. Мақалада Беларусь Республикасындағы ақпараттық қауіпсіздік пен киберқауіпсіздік мәселелерін реттейтін нормативтік құқықтық актілердің ережелерін талдау негізінде киберқауіпсіздікті қамтамасыз етудің ұлттық жүйесін қалыптастырудың алғышарттары мен ерекшеліктері, мемлекеттік органдар мен ұйымдардың міндеттері мен функциялары қарастырылады, қоғамдық қатынастардың осы саласын құқықтық реттеу тәсілдерін одан әрі жетілдіру бағыттары айқындалады.
Түйінді сөздер: ақпараттық қауіпсіздік; киберқауіпсіздік; ұлттық киберқауіпсіздік жүйесі; ақпараттық инфрақұрылым; кибершабуыл; киберқауіпсіздік; кибертерроризм, киберқауіпсіздік.

Annotation. The article, based on the analysis of the provisions of legal acts regulating the issues of information security and cybersecurity in the Republic of Belarus, examines the prerequisites for the formation and features of the national system of cybersecurity, tasks and functions of state bodies and organizations, defines the directions for further improvement of legal regulation approaches in this area of public relations.
Keywords: information security; cybersecurity; national cybersecurity system; information infrastructure; cyberattack; cyberincident; cyberterrorism, cyberresistance.

В настоящее время всеобъемлющее влияние информационной сферы на внутренние и внешние политические, социально-экономические и иные процессы не вызывает сомнения. Стремительное развитие информационно-коммуникационных технологий во многом определяет динамику развития общественных отношений, требующих надлежащего правового регулирования с целью реагирования на новые вызовы и угрозы, имеющие, как правило, трансграничный характер.

Соответственно, первостепенной задачей государства является обеспечение национальной безопасности, реализация национальных интересов, в том числе в информационной сфере.

Согласно положениям Концепции национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» (далее – Концепция национальной безопасности), информационная безопасность представляет собой состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1].

Концепция национальной безопасности определяет:

- основные национальные интересы в информационной сфере;
- внутренние и внешние источники угроз национальной безопасности в информационной сфере;
- основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз в информационной сфере.

Вместе с тем глобальные вызовы последних лет, актуализировали необходимость ревизии положений Концепции национальной безопасности, внедрение принципиально новых организационных механизмов обеспечения национальной безопасности республики, в том числе в информационной сфере. Следует отметить, что на данном этапе в Республике Беларусь организована работа по разработке нового документа концептуального характера в сфере обеспечения национальной безопасности.

В свою очередь, концептуальные основы обеспечения информационной безопасности Республики Беларусь заложены в Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» (далее – Концепция информационной безопасности) [2].

Концепция информационной безопасности:

- основывается на международных соглашениях о сотрудничестве в области обеспечения информационной безопасности;
- определяет информационную безопасность как обособленный феномен и нормативный институт, по сути, признавая таковую в качестве новой сферы общественных отношений;
- закрепляет основы государственной политики по защите национальных интересов в информационной сфере;
- учитывает как гуманитарный (в части приоритета реализации конституционных прав граждан), так и технологический (в части формирования национальной информационной инфраструктуры) аспекты;

- артикулирует целевые установки на соблюдение информационного суверенитета и информационного нейтралитета государства, сохранение традиционных устоев и ценностей.

Особое внимание в Концепции информационной безопасности уделено вопросам обеспечения безопасности информационной инфраструктуры, элементами которой являются национальный сегмент сети Интернет, критически важные объекты информатизации, государственные информационные системы. Впервые на законодательном уровне закреплены определения таких понятий, как «кибератака», «кибербезопасность», «киберинцидент», «кибертерроризм», «киберустойчивость» и др.

Необходимо подчеркнуть, что Концепция информационной безопасности в качестве отдельного структурного элемента содержит раздел, предусматривающий механизмы ее реализации. В частности, положения данного документа надлежит учитывать при подготовке проектов нормативных правовых актов и иных документов, таких как планы работы государственных органов и т.п. Также для целей реализации положений данной Концепции в ней обосновывается необходимость как целенаправленного взаимодействия между государственным сектором и коммерческими организациями в форме государственно-частного партнерства, так и участия Республики Беларусь в обеспечении международной информационной безопасности.

Необходимость практической реализации положений Концепции информационной безопасности, бесспорно, стала одной из предпосылок разработки и издания Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» (далее – Указ о кибербезопасности) [3]. Данный акт в настоящее время не вступил в силу (начало действия документа, за исключением отдельных положений, – 17 августа 2023 г.).

Целью правового регулирования названного документа определено повышение уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз. Соответственно, на государственном уровне потребовалось разработать и внедрить комплексный подход по обеспечению безопасности республики в информационной сфере в части регулирования вопросов контроля состояния кибербезопасности информационной инфраструктуры государства.

Актуальность работы по созданию на национальном уровне эффективной системы обеспечения кибербезопасности, определения элементов и задач этой системы объясняется важностью превенции кибератак на информационные системы органов государственного управления, государственных организации и критическую

информационную инфраструктуру Республики Беларусь, возникновения рисков и угроз национальным интересам в информационной сфере.

Следует отметить, что при подготовке проекта Указа о кибербезопасности его разработчиками учитывался зарубежный опыт, главным образом Российской Федерации (в силу наиболее тесного взаимодействия в рамках Союзного государства Республики Беларусь и Российской Федерации). В частности, в Российской Федерации создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак [4, 5, 6].

Указом о кибербезопасности определен уполномоченный государственный орган, координирующий деятельность государственных органов и иных организаций по созданию и обеспечению функционирования национальной системы обеспечения кибербезопасности, обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры.

Основной организационно-технической составляющей национальной системы обеспечения кибербезопасности стали особые субъекты: центры кибербезопасности и реагирования на киберинциденты. Соответствующие субъекты создаются на национальном уровне (Национальный центр обеспечения кибербезопасности) и на уровне государственных органов и иных организаций.

Основной задачей центров кибербезопасности является перманентный автоматизированный сбор, обработка, накопление, систематизация и хранение данных о кибербезопасности объектов информационной инфраструктуры, в том числе мероприятий по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов на этих объектах, а также реагированию на киберинциденты.

Обязанность по созданию центров кибербезопасности в первую очередь возложена на владельцев критически важных объектов информатизации, определенных Указом о кибербезопасности, поставщиков интернет-услуг, оказывающих услуги хостинга.

Издание данного Указа Президента Республики Беларусь отвечает требованиям современных реалий в части необходимости формирования единой системы кибербезопасности на государственном уровне. Вместе с тем полагаем, что его положения могут быть в дальнейшем усовершенствованы, посредством формирования правовых и организационных механизмов экстренного реагирования органов уголовного преследования на факты кибератак и вызываемые ими киберинциденты, являющиеся уголовно наказуемыми деяниями. Полагаем, что такая мера, как включение в данную систему (помимо специализированных государственных структур) Министерства внутренних дел Республики Беларусь (государственного органа,

имеющего в своей структуре специальные подразделения по борьбе с киберпрступностью) и наделение его полномочиями по предотвращению и минимизации последствий являющихся противоправными деяниями кибератак и киберинцидентов, будет способствовать более полному достижению целей правового регулирования.

Рассматривая вопросы обеспечения кибербезопасности, следует обратить внимание на соответствующую практику правового регулирования одной из наиболее проблемной в контексте настоящего исследования сфер – банковской сфере.

Так, в Национальном банке Республики Беларусь создан центр мониторинга и реагирования на компьютерные угрозы в банковской сфере Республики Беларусь. Кроме того, постановлением Правления Национального банка Республики Беларусь от 20 ноября 2019 г. № 466 утверждена Концепция обеспечения кибербезопасности в банковской сфере (далее – Концепция) [7]. Концепция является документом, разработанным на основе результатов анализа текущей ситуации, в том числе международной практики, в области обеспечения кибербезопасности банков, небанковских кредитно-финансовых организаций, открытого акционерного общества «Банк развития Республики Беларусь». Концепция отражает перспективные направления решения имеющихся и предотвращения вероятных проблем в сфере обеспечения кибербезопасности в банковской сфере.

Основной целью Концепции является формирование единообразного понимания и подходов к обеспечению кибербезопасности для устойчивого функционирования банковской сферы. Отметим, что данная цель является оправданной, поскольку должна предполагать распространение единого подхода на всех без исключения субъектов банковской сферы.

Необходимость выработки такого подхода, помимо прочего, обусловлена:

- существенным увеличением объемов предоставляемых банками цифровых финансовых услуг, как следствие, возрастание присущего такой деятельности риска, в том числе в части киберугроз;
- установлением новых банковских практик;
- процессами интеграции банковских сфер Республики Беларусь и государств – участников Евразийского экономического союза;
- санкционным давлением со стороны ряда зарубежных государств, затрагивающим банковскую сферу.

Кроме того, в положениях Концепции подчеркивается, что успешность кибератак, совершаемых в банковской сфере, во многом определяется человеческим фактором. Об этом свидетельствует постоянная практика использования в противоправной деятельности и совершенствования методов социальной инженерии. Концепция

содержит анализ типов кибератак и методов их осуществления, а также формулирует перспективные направления противодействия им.

Совершенствование методологии противодействия кибератакам в банковской сфере предполагает разработку пакета стандартов информационной безопасности, включающего, помимо прочего, требования:

- к системам управления кибербезопасностью;
- по обеспечению кибербезопасности при использовании технологий виртуализации;
- по управлению киберриском;
- по оценке соответствия кибербезопасности субъектов банковской сферы требованиям стандартов;
- по документационному обеспечению деятельности в области обеспечения кибербезопасности в соответствии с требованиями стандартов;
- управлению киберугрозами и киберинцидентами;
- по обеспечению кибербезопасности мобильных программных продуктов (мобильных приложений).

Следует отметить, что соответствующая работа в республике уже начата и результатом которой на данный момент является принятие ряда постановлений Правления Национального банка Республики Беларусь:

- от 26 августа 2022 г. № 316 «О представлении информации об инцидентах» [8] (определен порядок предоставления информации о совершенных операциях либо попытках совершения несанкционированных переводов денежных средств (электронных денег), фактах или попытках мошенничества в банковском секторе, а также о нарушениях безопасности и защиты информации, в том числе компьютерных атаках, направленных на объекты информационной инфраструктуры, которые могут привести к случаям и (или) попыткам осуществления несанкционированных переводов денежных средств (электронных денег);
- от 6 октября 2022 г. № 377 «Об утверждении Инструкции о требованиях по защите информации и обеспечению кибербезопасности при оказании платежных услуг» [9] (установлены требования по обеспечению защиты информации и кибербезопасности при оказании платежных услуг, а также требования по защите информации в платежных инструментах).

Резюмируя положения настоящего исследования, можно отметить следующее. В настоящее время в Республике Беларусь заложены правовые основы формирования национальной системы обеспечения кибербезопасности, что выразилось главным образом в подготовке и принятии ряда нормативных правовых актов концептуального характера. Кроме того, такие документы подвергаются корректировке с учетом

динамики развития и специфики соответствующих общественных отношений.

Разрабатываемая Концепция национальной безопасности призвана стать фундаментом проводимой работы, в том числе в сфере обеспечения информационной безопасности государства. Как представляется, данный документ обязательно должен предусматривать эффективные механизмы реализации его положений.

Нормами Указа о кибербезопасности заложены основы функционирования национальной системы обеспечения кибербезопасности. Вместе с тем перспективы необходимости совершенствования данного нормативного правового акта просматриваются уже в настоящее время.

Исходя из специфики сферы деятельности, одним из «пионеров» в части правового регулирования обеспечения кибербезопасности в Республике Беларусь становится банковская сфера. Принятие документа концептуального характера позволило обозначить не только существующие проблемные моменты деятельности субъектов банковских отношений, но и основные направления их решения. Полагаем, что сопоставимый подход целесообразен к применению и в законодательстве, регулирующим иные сферы общественных отношений.

Список использованных источников:

1. Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

2. Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

3. Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

4. Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2023.

5. Указ Президента Российской Федерации от 12 декабря 2014 г. № К 1274 «О Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2023.

6. Указ Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2023.

7. Постановление Правления Национального банка Республики Беларусь от 20 ноября 2019 г. № 466 «Об утверждении Концепции обеспечения кибербезопасности в банковской сфере» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

8. Постановление Правления Национального банка Республики Беларусь 26 августа 2022 г. № 316 «О представлении информации об инцидентах» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

9. Постановление Правления Национального банка Республики Беларусь от 6 октября 2022 г. № 377 «Об утверждении Инструкции о требованиях по защите информации и обеспечению кибербезопасности при оказании платежных услуг» // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СУДЕБНОЙ И ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

СОТ ЖӘНЕ ҚҰҚЫҚ ҚОРҒАУ ҚЫЗМЕТІНДЕ ЖАСАНДЫ ИНТЕЛЛЕКТТІ ҚОЛДАНУ МӘСЕЛЕЛЕРІ МЕН ПЕРСПЕКТИВАЛАРЫ

PROBLEMS AND PROSPECTS OF USING ARTIFICIAL INTELLIGENCE IN JUDICIAL AND LAW ENFORCEMENT ACTIVITIES

УДК 343.98:347.948

Абдолла Сакен Жусипахметович
Председатель Союза судей Республики Казахстан,
кандидат юридических наук, профессор,
г. Астана, Республика Казахстан

О ПЕРСПЕКТИВАХ ВНЕДРЕНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В СУДОПРОИЗВОДСТВО

Аннотация. Рассмотрены отдельные вопросы современного состояния использования инновационных технологий в судопроизводстве, в частности, в судебной экспертизе. Показано, что для повышения качества судопроизводства на современном этапе необходимо повысить эффективность судебно-экспертной деятельности путем развития перспективных направлений судебных экспертиз. Рассмотрены роды и виды судебных экспертиз, в которых используются и разрабатываются высокотехнологичные средства и методы исследования. Предложены рекомендации по внедрению самых передовых экспертных технологий в молекулярно-генетическую, психофизиологическую, компьютерно-техническую и другие виды и роды судебных экспертиз.
Ключевые слова: судебная экспертиза; инновационные технологии; методика; обеспечение; эксперт; судебно-экспертная деятельность.

Аннотация. Сот өндірісінде, атап айтқанда, сот сараптамасында инновациялық технологияларды қолданудың қазіргі жағдайының кейбір мәселелері қарастырылған. Қазіргі кезеңде сот ісін жүргізудің сапасын арттыру үшін сот сараптамаларының перспективалық бағыттарын дамыту арқылы сот-сараптама қызметінің тиімділігін арттыру қажет екендігі көрсетілген. Сот сараптамасының түрлері мен түрлері қарастырылады, оларда жоғары технологиялық құралдар мен зерттеу әдістері қолданылады және әзірленеді. Сот сараптамасының молекулярлық-генетикалық, психофизиологиялық, компьютерлік-техникалық және басқа да түрлері мен тектеріне ең озық сараптамалық технологияларды енгізу бойынша ұсынымдар беріледі.
Түйінді сөздер: сот сараптамасы; инновациялық технологиялар; әдістеме; қауіпсіздік; сарапшы; криминалистикалық қызмет.

Annotation. Some issues of the current state of the use of innovative technologies in legal proceedings, in particular, in forensic examination, are considered. It is shown that in order to improve the quality of legal proceedings at the present stage, it is necessary to increase the efficiency of forensic expert activity by developing promising areas of forensic examinations. The types of forensic examinations in which high-tech research tools and methods are used and developed are considered. Recommendations on the introduction of the most advanced expert technologies in molecular genetic, psychophysiological, computer-technical and other types of forensic examinations are proposed.
Keywords: forensic examination; innovative technologies; methodology; provision; expert; forensic expert activity.

Во многих странах мира, по статистическим данным, наблюдается достаточно сложная криминогенная обстановка, особенно, в сфере преступлений с использованием информационных и

телекоммуникационных технологий [1]. Это требует серьезных положительных действий со стороны правоохранительных органов, в том числе, путем повышения уровня научно-технического обеспечения судопроизводства. Особое внимание следует уделить высокотехнологичному экспертному сопровождению уголовных дел, связанных с терроризмом, выступающим «передним краем», внешним выражением, экстремизмом «на выходе» [2, с. 34].

Для повышения качества судопроизводства на современном этапе необходимо повысить эффективность судебно-экспертной деятельности путем развития перспективных инновационных направлений судебных экспертиз.

Судебно-экспертная деятельность, как система «действий руководителя, судебного эксперта судебно-экспертной организации, а также иных лиц – обладателей специальных знаний, привлеченных в качестве экспертов, по организации, производству, научно-методическому, информационному и материально-техническому обеспечению судебных экспертиз, выполняемых по поручению уполномоченного лица или органа, их назначившего, и экспертной профилактике» [3, с. 145] в настоящее время подвергается серьезному переформатированию, связанному с внедрением инновационных технологий во все направления.

Так, в судебно-экспертных организациях проводятся новые, в том числе инновационные, роды и виды судебных экспертиз: эстетическая [4], экспертиза объектов фалеристики (государственных наград: орденов и медалей), гидроэкологическая [5], палинологическая экспертиза с установлением характерных фитолитов, психолого-лингво-фоноскопическая, экспертиза по установлению компьютерного монтажа документов и другие.

Активизируется международный обмен экспертными методиками: например, «в настоящее время зарубежными коллегами широко применяются разработанные российскими учеными методики производства лингвистических, судебно-баллистических экспертиз; в то же время российские судебные эксперты с интересом изучают опыт производства религиоведческих экспертиз в Республике Казахстан» [6, с. 12].

Успешно проводятся высокотехнологичные судебные экспертизы по идентификации человека по функциональному признаку – походке.

В настоящее время в стадии внедрения находятся компьютерные программные комплексы исследования мобильных устройств с разрушенными носителями; компьютерные конструкторы осмотров мест происшествий в 3Д-формате; компьютерные программные комплексы по использованию БПЛА в следственных действиях и оперативно-розыскных мероприятиях; установление с помощью искусственного

интеллекта комплекса свойств неустановленного преступника по следам преступления и т.д.

Особенным является то, что для усиления качества инновационных методов исследования большую положительную роль выполняет разработанная Е.Р. Россинской в составе учения о цифровизации судебно-экспертной деятельности «система информационно-компьютерного обеспечения судебно-экспертной деятельности, как методологическая и технологическая основа использования IT-технологий в экспертных исследованиях любых объектов судебной экспертизы» [7, с. 264]. Поэтому крайне важно, чтобы такие инновационные методы, как «разработанный учеными-генетиками Института биохимии и генетики Уфимского Федерального исследовательского центра Российской академии наук (УФИЦ РАН) оригинальный метод оцифровки в бинарном формате сразу всей четверки нуклеотидов в каждом «снипе»[8], позволяющий проводить детекцию более коротких участков ДНК в старых биологических образцах» [8, с. 423], были в кратчайшие сроки внедрены в практику борьбы с преступностью. При использовании таких методов достигается максимальная цифровизация: «объем информации при ДНК-идентификации личности с помощью снипов составит для одного человека не более одного килобайта (для сравнения: с помощью ныне практикуемых STR-локусов – более 200 килобайт)» [9, с. 97].

Таким образом, применение инновационных технологий, разработанных учеными-генетиками г. Уфы, позволяет отойти от подходов, основанных на STR-локусах, предлагаемых фирмами США. К тому же, инновационные молекулярно-генетические технологии являются менее дорогостоящими и позволяют решать многие проблемы, связанные с идентификацией личности в результате проверки по системе геномной регистрации, что, в свою очередь, ведет к повышению качества расследования преступлений и судопроизводства в целом.

Применение вышеуказанных инновационных технологий молекулярно-генетической экспертизы позволяет, по данным уфимских ученых-криминалистов, достичь положительных результатов в борьбе с преступностью при исследовании еще одной значимой группы объектов. Так, известно, что на одежде граждан, содержащих кошек и собак, имеется шерсть этих животных. Таким образом, при физическом контакте преступника и жертвы часть таких шерстинок может переноситься с одежды одного на одежду другого человека. Получается, что если преступник в своем жилище имеет кошку или собаку, то вполне вероятно, что их шерсть перейдет на одежду жертвы. И тогда, выделив из них ДНК с помощью вышеописанного инновационного метода, можно

[8] Снип – SNP (Single-Nucleotide Polymorphism) – участок ДНК, последовательности аллелей которого различаются одним нуклеотидом.

будет установить конкретное животное и, соответственно лицо (хозяина животного), причастное к совершению преступления [10, с. 59-60].

Имеются хорошие перспективы развития и других инновационных методов экспертных исследований. Так, специалисты из Нижнего Новгорода (В.А. Юматов, П.Г. Лесникова) в результате авторских разработок внедрили в судебную почерковедческую экспертизу методы математического моделирования с программным обеспечением кодирования письменных знаков [11, с. 24]. Проводится идентификация личности по динамическим признакам человека (например,походке), запечатленным на цифровом носителе с помощью камер видеонаблюдения – судебная видеопортретная экспертиза.

Перспективным направлением следует признать и психофизиологическую экспертизу с применением полиграфа. В развитии этого вида исследования проведены серьезные методические разработки российскими полиграфологами: Юрием Ивановичем Холодным, Ярославой Владимировной Комиссаровой, Александром Петровичем Сошниковым. Серьезные исследования по методическому обеспечению этой экспертизы проводит их коллега из Республики Казахстан Сергей Юрьевич Алесковский. Необходимо проведение серьезной валидации с последующей сертификацией научно-обоснованной методики данного вида судебной экспертизы.

Примеров перспективных направлений внедрения инновационных технологий в судопроизводство можно привести множество. В настоящее время особенное значение придается одному из самых актуальных направлений в этой сфере – применению искусственного интеллекта в судопризводстве, как искусственно моделируемой интеллектуальной деятельности человека (в нашем случае – судьи, следователя, эксперта и других участников судопроизводства).

По нашему мнению, перспективы внедрения инновационных технологий, включая искусственный интеллект, в судопроизводство будут реализовываться гораздо быстрее путем организации и систематического проведения научно-практических форумов для ознакомления с ними: съездов, симпозиумов, конференций, семинаров и других мероприятий по вопросам судебно-экспертной деятельности, с приглашением ведущих практикующих ученых-экспертов для проведения мастер-классов.

По нашему мнению, настало время практического решения проблем фундаментальных разработок и реального внедрения инновационных технологий в судебно-экспертную деятельность и в судопроизводство в целом.

Список использованных источников:

1. Состояние преступности в России за январь-декабрь 2021 года. . [Электронный ресурс] – Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/28021552 (дата обращения: 02.04.2022 г.).

2. Варданян А.В., Кулешов Р.В. О классификации явлений экстремизма и терроризма: единство сущности и поливариантность отображения в социуме // Правовое государство: теория и практика. 2015. № 4 (42). С. 31–35.

3. Аминев Ф.Г. О современном понятийном аппарате судебной экспертологии // Вестник Восточно-Сибирского института МВД России. 2017. № 4. С. 143-148

4. Бондаренко Л.К. Эстетическая экспертиза – предпосылки и перспективы развития // Дискуссионные вопросы теории и практики судебной экспертизы: материалы международной научно-практической конференции, посвященной памяти Т.В. Аверьяновой. РГУП, 25-26 марта 2021 г. М., РГУП, 2021. С. 113-115.

5. Васин Д.Ю. К вопросу об общих задачах судебных землеустроительных, экологических и гидрологических экспертиз // Дискуссионные вопросы теории и практики судебной экспертизы: материалы международной научно-практической конференции, посвященной памяти Т.В. Аверьяновой. РГУП, 25-26 марта 2021 г. М., РГУП, 2021. С. 147-156.

6. Аминев Ф.Г. О необходимости постоянного совершенствования организационно-правового и методического обеспечения судебно-экспертной деятельности // Вестник Академии правоохранительных органов. №4 (26). 2022. С. 8-15.

7. Россинская Е.Р. Учение о цифровизации судебно-экспертной деятельности в системе частных теорий судебной экспертологии // Теория и практика судебной экспертизы в современных условиях: материалы VIII Международной научно-практической конференции. МГЮУ, 28-29 января 2021 г. С. 261-267.

8. Аминев Ф.Г., Аминев А.Ф. О перспективах цифровизации ДНК-регистрации населения России // Судебная экспертиза как элемент защиты прав и законных интересов граждан и юридических лиц – Роль права в обеспечении благополучия человека: сборник докладов XI Московской юридической недели, 24.11. 2022: в 5 ч. Ч. 4. М.: Издательский центр Университета имени О.Е. Кутафина (МГЮА), 2022. С. 421-424.

9. Аминев Ф.Г. О необходимости принятия федерального закона «О всеобщей геномной регистрации в Российской Федерации» в целях улучшения качества раскрытия и расследования преступлений // Правовое государство: теория и практика. Уфа, 2019. № 3 (57). С. 94-98.

10. Аминев Ф.Г., Гарафутдинов Р.Р., Гиниятов Ю.Р., Чемерис А.В. Полиморфизм ДНК кошек и собак, выделенной из их шерсти, как элемент доказательственной базы при расследовании преступлений // Теория и практика фундаментальных и прикладных исследований в сфере судебно-экспертной деятельности и ДНК-регистрации населения Российской Федерации: материалы Международной научно-практической конференции (13–14 октября 2022 г.) / отв. ред. Ф.Г. Аминев. Уфа: НИИ НППГ, 2022. С. 59-63.

11. Аминев Ф.Г., Аминев А.Ф. О современных возможностях использования специальных знаний в расследовании преступлений // Национальные и международные тенденции и перспективы развития судебной экспертизы: сборник докладов Научно-практической конференции с международным участием, г. Нижний Новгород, 19–20 мая 2022 г. Нижний Новгород: ННГУ, 2022. С. 20-26.

12. Аминев Ф.Г. К вопросу реформирования судебно-экспертной деятельности в Российской Федерации // Криминалистика: теория и практика. [Электронный ресурс] – Режим доступа: материалы VIII Международной научно-практической конференции. Краснодар: Краснодарский университет МВД России, 2020. С. 57-62.

УДК 343.48:004

Аминев Фарит Гизарович
доктор юридических наук, профессор,
профессор кафедры криминалистики Института права ФГБОУ ВО
«Уфимский университет науки и технологий», г. Уфа;
профессор кафедры судебно-экспертной деятельности
ФГКОУ ВО «Краснодарский университет МВД России»,
академик РАЕН, заслуженный юрист Республики Башкортостан,
г. Краснодар, Член Президиума» Палата судебных экспертов имени
Ю.Г.Корухова (СУДЭКС)», г. Москва**,** Российская Федерация

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ ФОРМИРОВАНИЯ И ИСПОЛЬЗОВАНИЯ БОЛЬШИХ ДАННЫХ (BIG DATA) В СУДОПРОИЗВОДСТВЕ

Аннотация. В статье рассмотрены направления использования высоких технологий в судопроизводстве. В статье показано, что в практическую деятельность успешно внедряются компьютерные программные комплексы анализа больших данных (Big Data) на базе нейронных сетей в целях определения модели и цвета автомобиля, типа, размеров перевозимого груза, отслеживания разыскиваемых транспортных средств, установления психофизиологического портрета неизвестного преступника по различным видам оставленных им следов и т.д. В один ряд с прорывными направлениями, используемыми в судопроизводстве, следует поставить внедрение молекулярно-генетических технологий в деле использования базы данных ДНК. Показаны организационно-правовые проблемы использования больших данных (Big Data). Разработаны и предложены меры по организационно-правовой регламентации использования Big Data в правоприменительной практике.
Ключевые слова: большие данные; программное обеспечение; цифровизация; технология; базы данных; нейронные сети.

Аннотация. Мақалада сот өндірісінде жоғары технологияларды қолдану бағыттары қарастырылған. Мақалада машинаның моделі мен түсін, тасымалданатын жүктің түрін, өлшемін анықтау, іздестіруде жүрген көліктерді қадағалау, анықтау үшін нейрондық желілерге негізделген үлкен деректерді (Үлкен деректер) талдауға арналған компьютерлік бағдарламалық қамтамасыз ету жүйелері тәжірибеге сәтті енгізілгені көрсетілген. белгісіз қылмыскердің психофизиологиялық портреті оның қалдырған іздерінің алуан түріне және т.б. ДНҚ деректер базасын пайдалануда молекулярлық-генетикалық технологияларды енгізуді сот ісін жүргізуде қолданылатын серпінді салалармен бір қатарға қою керек. Үлкен деректерді (Big Data) пайдаланудың ұйымдастырушылық және құқықтық мәселелері көрсетілген. Құқық қолдану тәжірибесінде үлкен деректерді пайдалануды ұйымдастырушылық-құқықтық реттеу бойынша шаралар әзірленді және ұсынылды.
Түйінді сөздер: үлкен деректер; бағдарламалық қамтамасыз ету; цифрландыру; технология; дерекқор; нейрондық желілер.

Annotation. The article considers the directions of using high technologies in legal proceedings. The article shows that computer software systems for big data analysis (Big Data) based on neural networks are successfully implemented in practice in order to

determine the model and color of the car, the type and size of the cargo being transported, tracking wanted vehicles, establishing a psychophysiological portrait of an unknown criminal by various types of traces left by him, etc. The introduction of molecular genetic technologies in the use of the DNA database should be put on a par with the breakthrough directions used in legal proceedings. The organizational and legal problems of using big data are shown. Measures have been developed and proposed for the organizational and legal regulation of the use of Big Data in law enforcement practice.

Keywords: big data, software; digitalization; technology; databases; neural networks.

В условиях сложной криминогенной ситуации во многих странах мира, преступность, как тесно вплетенное в земную цивилизацию явление, впитывает и реализует в своей негативной деятельности все имеющиеся достижения человечества. Интенсивность этого процесса особенно наглядно просматривается в современную эпоху цифровизации. В преступных экономических, социально-политических, военных целях используются новейшие высокотехнологичные средства: начиная от совершения преступлений с помощью дистанционных технологий до использования технологий нейронных сетей и искусственного интеллекта.

Так, анализируя характеристику состояния преступности в 2022 году, представленную в официальной отчетности, можно заметить, что из 1 966 795 преступлений, зарегистрированных на территории Российской Федерации в январе-декабре 2022 года, 522 065 преступлений совершено с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 0,8 % больше показателей предыдущего года [1] (при этом, еще больше правонарушений остались латентными). Раскрываемость таких преступлений составила всего 27,2%. Расследование трех из четырех возбужденных по таким фактам уголовных дел приостанавливается по ч. 1 ст. 208 УПК Российской Федерации: из-за неустановления лиц, подлежащих привлечению в качестве обвиняемых. К сожалению, преступность опережает правоохранительные органы в умении и компьютерно-техническом оснащении. Поэтому остается неизвестной для следствия большая часть компьютерных хакеров, в том числе: «маклеров» (биржевых мошенников), «фрикеров» (телефонных мошенников), «кардеров» (мошенников, работающих с пластиковыми кредитными картами), «спуферов» (взломщиков защиты чужих компьютеров), «кракеров» (взломщиков кодов пластиковых карт покупателей сети Интернет), разработчиков вирусных программ, электронных шантажистов и других.

В этой ситуации правоохранительные органы и судебная система должны предпринять решительные меры в использовании инновационных цифровых технологий в борьбе с преступностью. Одним из перспективных направлений, по нашему мнению, является использование Big Data (больших данных), представляющих собой

колоссальные массивы информационных данных, постоянно накапливающихся, обновляющихся и обрабатываемых в скоростном режиме (персональные сведения социальных сетей, данные с измерительных устройств, приборов аудио- и видеорегистрации, банковские операции и т.д.). Для анализа больших данных используются высокотехнологичные средства и методы: искусственные нейронные сети, распознавание образов, машинное обучение, статистический анализ, моделирование и т.д.

Больший скачок использования Big Data в правоприменительной практике произошел в связи с началом объявленной в 2016 году четвертой индустриальной революции, которую Е.Р. Россинская еще ранее представила как «методологическую и технологическую основу использования IT-технологий в экспертных исследованиях любых объектов» [2, с. 264]. Так, в настоящее время правоохранительными органами России используется комплекс «Азимут-4» с компьютерным программным обеспечением на базе нейронных сетей в целях определения модели и цвета автомобиля, типа, размеров перевозимого груза, отслеживания розыскиваемых транспортных средств. Близка к окончанию разработка компьютерного программного комплекса по установлению с помощью нейросетей психофизиологического портрета неизвестного преступника по различным видам оставленных им следов и т.д.

В один ряд с вышеназванными и другими прорывными направлениями, используемыми в судопроизводстве, следует поставить внедрение молекулярно-генетических технологий в деле использования больших данных. В результате научных разработок удалось не только «прогнозировать будущее состояние здоровья и оценить риски возникновения патологических состояний» [3, с. 123], но и предложить осуществить всеобщую геномную регистрацию всего населения путем генетического штрих-кодирования на основе тетрааллельных снипов (SNP-локусов[9]), характеризующихся «наивысшим уровнем цифровизации (объем полученной таким способом генетической информации для одного человека равен не более 1 килобайта)» [4]. Разработана и зарегистрировано в Федеральной службе интеллектуальной собственности программное обеспечение по формированию, ведению и идентификации человека по базе данных ДНК [5]. Причем эти базы данных геномной информации (нейтральной информации, без возможности узнать что-либо о человеке, кроме его джин-кода) и только в целях ДНК-идентификации, введенных с помощью отечественных компьютерных программ и оборудования, будут содержаться в серверах, необходимое количество которых будет в 200

[9]SNP-локус (Single-NucleotidePolymorphismlocus):Участок ДНК, последовательности аллелей которого различаются одним нуклеотидом.

раз меньше, чем количество серверов, используемых «сейчас в России американской системой CODIS на базе STR-локусов» [6, с. 197].

Однако, меры правоохранительных органов по анализу и использованию Big Data в настоящее время явно недостаточны. Причем, предпринимаемые попытки государственного контроля над информацией в сетях Интернет и их использования в целях расследования и, в целом, для судопроизводства являются неподготовленными и явно ограниченными. Так, предложение Генеральной прокуратуры Российской Федерации в 2008 году о необходимости контроля над информационными потоками (по аналогии с Китайской Народной Республикой) российского сегмента Интернета встретило серьезное возражение со стороны пользователей Сети, и было интерпретировано «как посягательство на личную свободу» [7, с. 133].

В то же время, такое замедление организации широкого использованием больших данных в интересах судопроизводства создает усугубление следующих организационных проблем:

- затруднение анализа больших данных;
- неточное прогнозирование развития преступных правонарушений;
- отсутствие эффективных моделей государственного реагирования на криминогенную ситуацию в целях предупреждения преступлений и т.д.

Полагаем, что особое внимание должно быть уделено вопросам формирования и использования больших данных (Big Data) в судопроизводстве. Поэтому актуальными являются научные исследования и разработки инновационных средств и методов на базе цифровых технологий, включая искусственный интеллект, по обработке и использованию Big Data в практической деятельности, с их последующей организационно-правовой регламентацией. Для этого необходимо предпринять следующие меры:

1. Разработать организационно-правовые основы использования Big Data в целях полной легитимизации применения больших данных в деле решения актуальных прикладных задач судопроизводства, включив в них положения по этическим требованиям, которые регламентируют формирование и использование больших данных (в том числе, базы данных всеобщей геномной регистрации населения страны). Особое внимание в организации и правовом обеспечении этого направления должно быть уделено регламентации соотношения решений процессуально уполномоченных субъектов судопроизводства и результатов высокотехнологичного анализа больших данных (Big Data), произведенного при помощи программного обеспечения и компьютерных средств.

2. Разработать и включить в программы профессиональной

подготовки следователей, оперуполномоченных, судебных экспертов, а также в системе повышения квалификации судей нового раздела информационной подготовки – «Криминалистические средства и методы использования больших данных (Big Data)», позволяющего сотрудникам правоохранительных органов, в том числе, судьям, в последующей своей работе актуализировать информацию на базе изучения соответствующих источников и применять их в своей деятельности.

3. Нужно разработать экспертные системы, базирующиеся на когнитивных вычислениях, имеющих свойства самообучения, в том числе с использованием известных образцов программного обеспечения NoSQL, MapReduce, Hadoop и нейросетей. К выполнению этой задачи нацеливает ст. 23 Указа Президента России № 490 от 10 октября 2019 года «О развитии искусственного интеллекта в Российской Федерации» (в части обеспечения национальной безопасности и правопорядка). Для проведения такой работы, конечно же, должны выделяться определенные денежные и кадровые ресурсы.

4. Необходимо поднять уровень материально-технического обеспечения использования больших данных за счет приобретения (или собственного производства) суперкомпьютеров класса Summit от IBM, Fujitsu (Япония).

5. Необходимо создать в системе правоохранительных органов, включая суды, высококвалифицированные подразделения по использованию возможностей больших данных (Big Data) и обеспечить техническую возможность их доступа к таким базам данных.

6. Для успешного внедрения инновационных методов исследования следует повысить уровень профессиональной подготовки сотрудников правоохранительных органов, у которых должно быть гармоничное сочетание высокого уровня квалификации в конкретном виде деятельности с высоким уровнем знаний, умений и навыков в сфере компьютерных технологий.

7. Необходимо объединить усилия государств по тесному взаимодействию правоохранительных органов в деле использования больших данных в судопроизводстве (начиная с международного розыска преступников и без вести пропавших лиц и заканчивая борьбой с организованной киберпреступностью) с соответствующим международным организационным оформлением и нормативно-правовым закреплением (принятием международных Конвенций, соглашений и других нормативных правовых документов).

Только комплексный подход в организационно-правовой регламентации использования больших данных (Big Data) позволит повысить эффективность их применения в судопроизводстве.

Список использованных источников:

1. Состояние преступности в России за январь-декабрь 2022 года. [Электронный ресурс] – Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения: 20 марта 2023)

2. Россинская Е.Р. Учение о цифровизации судебно-экспертной деятельности в системе частных теорий судебной экспертологии // Теория и практика судебной экспертизы в современных условиях: материалы VIII Международной научно-практической конференции. МГЮУ, 28-29 января 2021 г. С. 261-267.

3. Хусаинова Р.И., Ахтямова Е.В., Минниахметов И.Р., Султанова Р.И. Современные молекулярно-генетические технологии в медицине: этнические и правовые вопросы // Правовое государство: теория и практика. Уфа, 2020. № 2 (60). С. 123-133.

4. Garafutdinov R.R., Sakhabutdinova A.R., Slominsky P.A., Aminev F.G., Chemeris A.V. A new digital approach to SNP encoding for DNA identification // Forensic Science International. 2020. V. 317. P. 110-520. DOI: 10.1016/j.forsciint.2020.110520.

5. Аминев Ф.Г., Сагитова М.А., Чемерис А.В., Гарафутдинов Р.Р., Сагитов А.М., Анисимов В.А. SNPmod: Свидетельство о регистрации программы для ЭВМ 2022683416 05.12.2002. Заявка № 2022683187 от 28.11.2022. Федеральная служба по интеллектуальной собственности, 2022.

6. Янгиров А.И. О возможностях методического обеспечения судебно-экспертной деятельности в условиях цифровизации // Юристъ-Правоведъ. № 1. 2023. С. 195-200.

7. Ищенко Е.П. Виртуальный криминал. Москва: Проспект, 2017. 232 с.

Ахметов Ерадиль Калидулович
Заместитель председателя
Комитета по правовой статистике и специальным учетам
Генеральной прокуратуры Республики Казахстан,
г. Астана, Республика Казахстан

доклад на тему:

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Технологии искусственного интеллекта (ИИ) все больше становятся частью нашей повседневности. Из разряда элементов научной фантастики они перешли в разряд составляющих во всех сферах жизни.

С развитием технологий искусственного интеллекта (ИИ) в правоохранительной деятельности появляются новые возможности для превентивной борьбы с преступностью и улучшения работы правоохранительных органов. Вот несколько перспектив внедрения ИИ в правоохранительную деятельность:

1. Анализ больших данных, что позволяет выявлять связи между преступлениями, распознавать преступников, выявлять уклонение от налогов, нарушения контрактов и другие правонарушения.
2. Увеличение скорости реакции: ИИ может помочь правоохранительным органам быстрее раскрывать преступления и проактивно предотвращать преступления на основе данных.
3. Улучшение качества решений: ИИ может использоваться для анализа доказательств и обеспечения более точных и эффективных решений в правоохранительной деятельности.
4. Улучшение безопасности: ИИ может быть применен для обнаружения угроз и предотвращения террористических актов, а также обеспечения безопасности публичных мероприятий.
5. Повышение эффективности правоохранительной деятельности: Использование ИИ позволит правоохранительным органам эффективнее распределять ресурсы и улучшить оперативную деятельность.

Всемирный тренд по внедрению технологий искусственного интеллекта (далее – ИИ) предполагает неизбежность внедрения технологий в правоохранительную деятельность. Необходимость оперативного и качественного анализа получаемых данных о расследуемом правонарушении, оперативности принятии решений по ним. Эти обстоятельства приводят нас к внедрению технологий ИИ в деятельность по составлению рутинных документов, при реализации полномочий сотрудниками правоохранительных органов и к экономии трудового процесса.

Цифровая трансформация в правоохранительной сфере обусловлена растущими требованиями к сотрудникам при решении задач по расследованию и раскрытию преступлений. Необходимости в обработке и управлении большим массивом накопленных данных о преступлениях, которые крайне затруднительно обработать человеческим мозгом.

Поэтапная интеллектуализация цифровых технологий, используемых в правоохранительной сфере при составлении процессуальных документов, не только позволяет сократить временной ресурс для решения вопросов, требующих сложного аналитического подхода в их составлении, но и открывает новые возможности, что повысит эффективность деятельности сотрудников в целом.

Преимуществами технологий, использование которых основано на применении ИИ при составлении процессуальных документов, являются возможность накопления, сбора данных под определенные целевые задачи, возможность построения алгоритмов для принятия решения и составления документов, возможность генерации процессуальных документов, обусловленных индивидуальными особенностями уголовного дела.

Так, Комитетом реализована автоматизированная база данных «Единый реестр досудебных расследований» предназначенная для регистрации уголовных правонарушений, расследования уголовных дел (в том числе в электронном формате), прокурорского надзора за ходом досудебного расследования и направления уголовных дел в суд.

ЕРДР введен в промышленную эксплуатацию в 2018 году, прошла испытания на соответствие требованиям информационной безопасности.

На его базе создан функционал «Е-уголовное дело» (Е-УД), который позволяет расследовать и рассматривать дела в суде в электронном формате.

В целом хотелось бы отметить, что с 2018 года доля дел, расследованных в электронном формате, увеличилась с 5% до 90,8% в 2022 году (175 258). Из них более 29 тыс. дел (28 958) направлено в суд.

Преимущества электронного производства:

- автоматизация и оперативность сбора данных о преступлениях, результатах расследования уголовных дел и привлечения к ответственности виновных лиц;

- исключение рисков фальсификаций и коррупционных проявлений.

- упрощение процедур согласования и формирования шаблонов процессуальных документов;

- назначение судебных экспертиз с получением результатов в электронном формате;

- возможность получения копий процессуальных документов через информационный портал «Публичный сектор»;

- автоматизированное назначение адвокатов в рамках гарантированной государством юридической помощи «Е-Заң көмегі»;

- полнота, объективность и достоверность правовой статистики и другое.

На основе накопленного цифрового массива данных о расследуемых уголовных делах, поэтапно внедряем элементы искусственого интелекта.

Так, в рамках электронного уголовного дела внедряется интеллектуальный помощник следователя, который будет подсказывать какую статью уголовного кодекса выбрать, какое провести следственное действие, какое решение принять и т.д.

Также, будем совершенствовать функционал «Заңдылық» подсказывающий прокурорам какую меру наказания по какой статье необходимо назначить с учетом всех процессуальных моментов, формирует обвинительную речь гособвинителя.

В части административного процесса также мы видим перспективы внедрения технологий ИИ. Применение сплошного видеонаблюдения на дорогах позволило в автоматическом режиме составлять предписания при выявлении нарушений.

Также распознается не только гос.номер, но и габариты грузовых автомобилей.

Фиксируются автотранспортные средства с просроченным техосмотром или страховкой, с неуплаченными штрафами, а также находящиеся в угоне, в розыске или с подложными гос.номерами.

К примеру, при нарушении скоростного режима система фиксирует правонарушение, распознает номер транспортного средства, запрашивает сведения из баз данных о правонарушителе (его анкетные данные, место работы, номер телефона, наличие водительского удостоверения, страховки и др.), затем формирует предписание, подписывает его и направляет нарушителю уведомление. Т.е. все это делается без участия сотрудника полиции. Мы работаем над тем чтоб система автоматически выявляла все нарушения, там где они были. Накопленный огромный массив нарушений, в том числе с фото и видеофиксацией позволяет обучать систему, чтоб исключать те факты, где к примеру нарушение было связано с объездом препятствия на дороге.

В дальнейшем, это позволит упростить составление процессуальных документов, снизятся материальные затраты и нагрузки на правоохранительные и судебные органы, минимизируются риски фальсификации материалов дел.

Кроме распознавания машин, было бы полезно в правоохранительной деятельности широко применять технологии распознавания лиц. К примеру, по розыску скрывшихся преступников, на сегодня проводится пилотный проект, когда в общественных местах

видеокамеры позволяют распознавать входящих лиц и автоматически выявлять среди них разыскиваемых.

Также искусственный интеллект при анализе видеоизображения позволяет выявлять террористические угрозы, например, оставленные подозрительные предметы, нестандартное поведение людей и другие возможности. В сегодняшних реалиях, когда в крупных городах установленных десятки тысяч камер наблюдения, без применения видеоанализа, т.е. искусственного интеллекта, эффективность затрат значительно снижается.

Элементы ИИ внедряются при создании и использовании геоинформационных карт. Все уголовные правонарушения у нас отображаются на Карте, с разбивкой по видам, времени совершения и другим параметрам. Этот массив данных позволяет прогнозировать вероятность совершения преступления в том или ином месте, соответственно система позволит строить маршруты патрулирования, расстановку средств и сил полиции.

Аналогично и в профилактике аварийности на дорогах. Уже сейчас на карте мы видим наиболее аварийные участки дорог, какое количество ДТП там произошло, какие это ДТП, причины и условия, которые им способствовали. При правильном анализе система будет подсказывать принятие мер для снижения смертности и травматизма на дорогах.

Основные преимущества внедрения ИИ:

- экономия ресурсов и времени
- выявление скрытых правонарушений
- поиск неизвестных угроз
- моделирование новых угроз.

Внедрение ИИ окажет ощутимое влияние в работе правоохранительных органов, уменьшит участие в процессе человеческого ресурса, увеличит объем анализируемых данных в информационных системах. В итоге это приведет к повышению безопасности и правопорядка в стране.

УДК 004.8:34

Бахтеев Дмитрий Валерьевич,
Доцент кафедры криминалистики УрГЮУ имени В.Ф. Яковлева,
доктор юридических наук, доцент,
г. Екатеринбург, Российская Федерация

ОЦЕНКА ЭФФЕКТИВНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ НА ПРИМЕРЕ ПРОЕКТА NSP-SIGVER

Аннотация. В статье рассматриваются современные подходы к оценке эффективности систем искусственного интеллекта с позиций, допускаемых правильных и ошибочных решений, а также критериев точности, правильности и полноты. Данные критерии анализируется на примере проекта NSP-SigVer – системы верификации рукописной подписи. Делается вывод о том, что эффективность интеллектуальных систем должна зависеть от эффективности аналогичного направления человеческой деятельности, что подтверждается проведённым экспериментов по установлению точности определения подлога подписи человеком.

Ключевые слова: искусственный интеллект; машинное обучение; распознавание подписей; эффективность ИИ; рациональность; ошибки ИИ.

Аннотация. Мақалада жасанды интеллект жүйелерінің тиімділігін рұқсат етілген дұрыс және қате шешімдер, сондай-ақ дәлдік, дұрыстық және толықтық критерийлері тұрғысынан бағалаудың заманауи тәсілдері қарастырылады. Бұл критерийлер қолмен жазылған қолтаңбаны тексеру жүйесінің NSP-SigVer жобасының мысалында талданады. Интеллектуалды жүйелердің тиімділігі адам қызметінің ұқсас бағытының тиімділігіне байланысты болуы керек деген қорытынды жасалады, бұл адамның қолтаңбаның жалғандығын анықтаудың дәлдігін анықтау үшін жүргізілген эксперименттермен расталады.

Түйінді сөздер: жасанды интеллект; машиналық оқыту; қолтаңбаны тану, тиімділік және ұтымдылық; жасанды интеллекттің қателіктері.

Annotation. The paper considers current approaches to assessing the effectiveness of artificial intelligence systems from the perspective of correct and erroneous decisions allowed, as well as the criteria of accuracy, precision and recall. These criteria are analyzed on the example of the project NSP-SigVer – handwritten signature verification system. It is concluded that the effectiveness of intelligent systems should depend on the effectiveness of similar human activities, which is confirmed by the conducted experiments to determine the accuracy of human signature forgery.

Keywords: artificial intelligence; machine learning; signature recognition; effectiveness of AI; rationality; AI errors.

Поведение субъекта судопроизводства, равно как интеллектуальной системы, повышающей его эффективность должно подчиняться критерию рациональности. В когнитивных науках и экономике под рациональностью часто понимают две различные её формы.

Инструментальная рациональность – оптимизация достижения целей человеком. Показателем рационального поведения в этом случае будет величина его отклонения от паттерна оптимального выбора [1; 19–20]. Именно в ключе этого понимания критериев рациональности следует оценивать эффективность функционирования современных систем искусственного интеллекта.

Другим типом рациональности является эпистемическая (фактологическая) рациональность, под которой понимают соответствие убеждений субъекта структуре реального мира [2], [3], [4]. Полагаем, что реализация данного типа рациональности системой искусственного интеллекта позволит говорить о наличии у него самосознания и такую систему следует считать манифестацией сильного (общего) искусственного интеллекта. Зачастую к указанным двум типам добавляют ещё аксиологическую рациональность – систему целеполагания и производных от неё действий, направленных на достижение ценностного результата [5], [6]. Этот тип рациональности для понимания и оценки с его помощью прикладных и экспериментальных систем искусственного интеллекта (равно как и другого сложного технологического решения или комплекса решений) представляется слишком рискованным: вполне вероятна коллизия при сопоставлении интересов и ценностей пользователя системы и общества в целом.

Помимо рациональности – как качественного критерия – эффективность систем машинного обучения может быть оценена количественно – через совокупность качественных критериев, отражающих негативные и положительные стороны функционирования таких систем. Рассмотрим это более подробно.

В основе оценки эффективности систем машинного обучения лежит матрица ошибок – таблица комбинаций ответов системы относительно реальности. Выглядит она следующим образом:

Таблица 1. Матрица ошибок – возможные ответы системы

	Ответ соответствует реальности	Ответ не соответствует реальности
Положительный ответ	TP	FP
Отрицательный ответ	FN	TN

TP (true-positive, истинно-положительный) – положительное решение системы, точно соответствующее реальности, заданной при разметке данных. Приведём пример такого случая: система искусственного интеллекта (или же человек) считает, что в данном случае имеются полные основания для вынесения судебного приказа. Это решение не будет ни обжаловано, ни отменено. Если речь идёт, к

примеру, про распознавание подложных подписей – то в таком случае система правильно находит признаки подлога в подложной подписи.

TN (true-negative, истинно-отрицательный) – отрицательное решение системы, точно соответствующее реальности, заданной при разметке данных. В этом случае система искусственного интеллекта откажет в выдаче судебного приказа, что будет соответствовать и нормам права, и судебной ситуации, либо распознавание подлинной подписи именно в таком статусе.

Эти два решения с позиций эффективности являются оптимальными и соответственно, могут считаться целью как при разработке систем искусственного интеллекта, так и при оценке деятельности человека.

Помимо правильных решений, ни человек, ни машина не застрахованы от ошибок. В случае интеллектуальных систем ошибки чаще всего могут быть вызваны неоднородностью или иной некорректностью входных данных (датасета), либо же появиться в результате обобщения или переобучения сети. Под обобщением понимают чрезмерное упрощение сети, при котором она не воспроизводит мелкие зависимости и выдаёт всегда средние результаты. При переобучении искусственная нейронная сеть имеет излишне сложную структуру и слишком тщательно пытается соответствовать поставленным целям, «подгоняет» результаты, что выражается в существенной разнице между результатами обучения и валидации результатов обучения [7; с. 64]. Такие ошибки могут быть условно названы внутренними. В случае человека они обычно объясняются пробелами в знании, низким уровнем профессионализма, правосознания и т. д. Другая причина ошибок – внешние факторы, которые могут быть обусловлены умышленными противоправными действиями, ориентированными на введение системы искусственного интеллекта в заблуждение: это могут быть рисунки на лице для систем распознавания внешности, дополнительные символы на государственных номерах транспортных средств – для систем, подобным специального программного обеспечения «Паутина», способного идентифицировать признаки автомобилей, либо же скрытому тексту в документе – для систем, способных «читать» документы, в том числе юридические. Такие действия со стороны лиц, противодействующих интеллектуальным системам, называются состязательными атаками. Также отметим, что интеллектуальные системы обучаются на однородных данных и в настоящее время способны разрешать только простые, статистически частые ситуации, вследствие чего при возникновении сложных случаев система склонна совершать ошибки или прекращать работу, подобно тому, как человек подвержен ступору или панике. Ошибки определяются относительно исходной общей гипотезы, в нашем примере это: выдача судебного

приказа при наличии достаточных оснований, распознавание подложной подписи как подложной подписи. Ошибки, согласно приведённой таблице, также разделяются на два следующих вида.

FP (false-positive, ложноположительная) – положительное решение системы, при отрицательном правильном решении. Продолжая вышеуказанные примеры, судебный приказ в этом случае не будет выдан, хотя присутствуют должные основания его выдачи, а подлинная подпись будет воспринята как подложная. Есть основания считать, что в экспериментальных условиях при наличии актуализированной осведомлённости о возможности подлога, согласно проведённому нами изучению возможности распознавания человеком подлинности рукописной подписи, люди при оценочных решениях склонны к ошибкам именно такого рода [8; с. 76]. Такого рода ошибки исправляются за счёт затребования дополнительных ресурсов для оспаривания решения системы, к примеру, обжалования судебного решения или назначения судебной экспертизы спорной подписи. Количественный показатель таких ошибок (коэффициент ложного принятия (False Acceptance Rate, FAR) рассчитывается как отношение ложноположительных ошибок, разделённое на общее количество обработанных объектов (ситуаций).

FN (false-negative, ложноотрицательная) – отрицательное решение системы, при положительном правильном решении. При совершении такой ошибки, судебный приказ будет выдан в отсутствие необходимых юридических оснований, а подложная подпись будет воспринята как подлинная (соответственно, документ с признаками подлога будет считаться легальным). В случае таких ошибок система, неважно, идёт речь о суде, службе безопасности банка или следственном органе, не получит сигнал об ошибке, таким образом ложноотрицательные ошибки как человека, так и системы искусственного интеллекта имеют тенденцию к латентности. Количественный показатель таких ошибок (коэффициент ложного отклонения (False Rejection Rate, FRR) рассчитывается по аналогичной формуле: как отношение ложноотрицательных ошибок, разделённое на общее количество обработанных объектов (ситуаций).

Правильность (accuracy) является наиболее интуитивно понятной метрикой и описывается как доля правильных ответов системы в общем количестве ситуаций или вопросов, ей заданных, или же соответствие работы системы поставленным задачам. Вместе с тем, эта метрика используется редко, поскольку подходит исключительно для оценки равных классов. Если объём данных в разных ситуациях различается, то правильность перестаёт быть корректной характеристикой. Объясним это на примере: интеллектуальной системе предъявляется два набора данных: в первом содержатся 100 пар подлинных подписей, во втором – 10 пар подписей, в каждой паре из которых присутствует одна подложная подпись. Если система верно

распознает 90 подписей из первого набора (90 TN (подделка не выявлена), 10 FP (подделка выявлена (ложно)), и 5 подписей из второго набора (5 TP (подделка обнаружена) и 5 FN (система пропустила подделку), то формула правильности будет рассчитываться следующим образом:

$$\text{Правильность} = \frac{TP + TN}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} = \frac{5 + 90}{5 + 90 + 10 + 5} = 86{,}4\ \%$$

Системы искусственного интеллекта обучаются, стремясь достичь поставленных разработчиком результатов. Аналогично, при введении KPI в организациях часто главным стремлением сотрудников является достижение поставленных показателей, а не необходимых результатов деятельности. В описываемом примере система может, опираясь на больший набор данных, поднять свою правильность, размечая все предъявленные ей подписи как подлинные. Формула примет следующий вид.

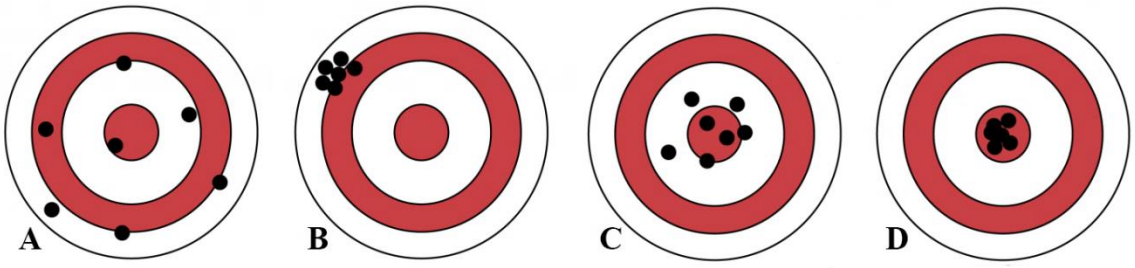
$$\text{Правильность} = \frac{TP + TN}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} = \frac{0 + 100}{0 + 100 + 0 + 10} = 90\ \%$$

В случае человеческой деятельности это обычно называется «подгонкой» результатов к необходимым статистическим показателям. Реальная полезность, очевидно, при этом падает.

Точность (precision) – доля положительных решений системы (правильных решений) относительно общего числа реальных положительных решений. Точность также может называться положительной предсказательной ценностью (positive predictive value (PPV)). Точность не позволяет системе принимать во всех случаях единственное решение (в этом случае за счёт роста FP точность будет падать).

$$\text{Точность} = \frac{TP}{TP + FP}$$

Взаимозависимость правильности и точности показана на Илл. 1.



Илл. 1. Соотношение точности (precision) и правильности (accuracy):
A: Низкая точность и низкая правильность;
B: Высокая точность и низкая правильность;
C: Низкая точность и высокая правильность;
D: Высокая точность и высокая правильность.
(Автор исходного изображения: Anni-Helena Ruotsala)

Помимо правильности и точности, в машинном обучении используются и другие метрики, к примеру **полнота (recall)** – доля истинно положительных решений системы, или

способность системы в принципе обнаруживать необходимые признаки в исследуемом объекте.

$$\text{Полнота} = \frac{TP}{TP + FN}$$

Для оценки интеллектуальной системы, принимающей большое количество решений (деятельность субъекта правосудия или правоприменения также может быть охарактеризована таким образом), следует применять указанные или схожие методы оценки эффективности. Эффективность машинных систем измерить достаточно несложно, однако если речь идёт хотя бы о частичном замещении машиной отдельных функций человека, то помимо определения условий использования и донесения этой информации до пользователей; информированности об опасностях и обязательного предварительного тестирования [9; с. 109–110], необходим комплекс операций по сравнению эффективности человека с позиций машинного обучения, то есть через описанные выше метрики. Так, в нашем эксперименте с распознаванием подложных подписей были использованы аналогичные показатели человека. Для этого было организовано специальное анкетирование в целях установления способности человека распознавать подлог подписи в официальном документе. Вероятность успешности такого действия напрямую зависит от опыта и специальной подготовки человека, а также качества самого подлога. Каждому из 256 респондентов предлагалась анкета, включавшая форму для сбора установочных показателей: пола; возраста; уровня образования; наличия подготовки в области почерковедения, исследования документов или смежных областях; субъективной самооценки собственных навыков респондента по выявлению подлога подписи. Далее предлагалось засечь время (анкета являлась хронометрируемой: выяснению подлежало также среднее время на сопоставление подписей), за чем следовал набор из 10 комплектов подписей, одна из которых была достоверно подлинная, а подлинность остальных четырёх нужно было попытаться установить на основе визуального сравнения подписей. По итогам анкетирования было установлено, что вероятность такого распознавания подлога подписей не превышает в среднем 69 %, соответственно, любые более высокие показатели разрабатываемой искусственной нейронной сети, уже являются примером работоспособности сети.

Список использованных источников:

1. Станович К.И. Рациональное мышление. Что не измеряют тесты способностей / пер. с англ. И. Ющенко. – М.: Карьера Пресс, 2016. – 334 с.

2. Audi R. The Architecture of Reason: The Structure and Substance of Rationality. – Oxford: Oxford University Press, 2001. – 304 p.;

3. Mele A.R. The Oxford Handbook of Rationality / A.R. Mele, P. Rawling. – Oxford: Oxford University Press, 2004. – 496 p.;

4. Колмакова Е.А. Гносеологическая и социокультурная специфика эпистемической и инструментальной рациональности: автореф. … дис. канд. филос. наук. – Омск: Омский государственный педагогический университет, 2008. – 19 с.
5. Лосский Н.О. Ценность и бытие. – М.: АСТ, Фолио, 2000. – 864 с.;
6. Выжлецов Г.П. Научная рациональность в эпоху аксиологического релятивизма // Вестник Санкт-Петербургского университета. Серия 17. Философия. Конфликтология. Культурология. Религиоведение. – 2015. – № 4. – С. 21–26.
7. Бессмертный И.А. Системы искусственного интеллекта: учеб. пособие для академического бакалавриата. – 2-е изд., испр. и доп. – М.: Издательство Юрайт, 2018. – 130 с.
8. Бахтеев Д. В. Искусственный интеллект: этико-правовые основы / Д.В. Бахтеев. – Москва: Общество с ограниченной ответственностью «Проспект», 2021. – 176 с.
9. Регулирование робототехники: введение в «робоправо». Правовые аспекты развития робототехники и технологий искусственного интеллекта / В.В. Архипов, В.В. Бакуменко, А.Д. Волынец [и др.]; под ред. А. В. Незнамова. – М.: Инфотропик Медиа, 2018. – 232 с.

УДК 341.492:004

Бертовский Лев Владимирович
профессор кафедры криминалистики Юридического факультета ФГБОУ ВО «Московский государственный университет им. М.В. Ломоносова», директор института высокотехнологичного права и социально-гуманитарных наук ФГАОУ ВО «Национальный исследовательский университет «Московский институт электронной техники», доктор юридических наук, профессор
г. Москва, Российская Федерация

ТЕХНОЛОГИЗАЦИЯ СУДОПРОИЗВОДСТВА

Аннотация. В статье указывается на логистичность, наукоемкость и технологичность современного права и делается вывод о необходимости создания цифрового судопроизводства. Представлены перспективы и проблемы развития технологизации современного судопроизводства и проблемы подготовки соответствующих специалистов в области права.
Ключевые слова: право; регулятор общественных отношений; высокие технологии; технологичности права; технологизация судопроизводства; информационные технологии; высокотехнологичное право; профессиональные компетенции; профессиональное обучение; социальные технологии.

Аннотация. Мақалада қазіргі заманғы құқықтың логистикасы, ғылымды қажетсінуі және технологиялылығы көрсетілген және цифрлық сот ісін жүргізу қажеттілігі туралы қорытынды жасалады. Қазіргі заманғы сот ісін жүргізуді технологияландыруды дамытудың перспективалары мен проблемалары және құқық саласындағы тиісті мамандарды даярлау мәселелері көрсетілген ұсынылған.
Түйінді сөздер: құқық; қоғамдық қатынастарды реттеуші; жоғары технологиялар; құқықтың технологиялығы; сот ісін жүргізуді технологияландыру; ақпараттық технологиялар; жоғары технологиялық құқық; кәсіби құзыреттер; кәсіптік оқыту; әлеуметтік технологиялар.

Annotation. The article points to the logistics, knowledge-intensive and technological nature of modern law and concludes that it is necessary to create digital legal proceedings. The prospects and problems of the development of the technologization of modern legal proceedings and the problems of training relevant specialists in the field of law are shown.
Keywords: law; regulator of public relations; high technologies; technological law; technologization of legal proceedings; information technologies; high-tech law; professional competencies; vocational training; social technologies.

Введение. Экспоненциальное развитие науки и техники, изменение социальных укладов и другие глубинные изменения, которые произошли за последнее время, выявили необходимость в значительной модернизации такого важного социального феномена, которым является право. Мы вступили в эпоху высокотехнологичного права, под которым

понимается логистичный[10], наукоемкий и технологичный регулятор общественных отношений, который, с одной стороны, использует высокие технологии в процессе правоприменения, а с другой – регламентирует возникающие с ними отношения[11].

Мировой опыт показывает, что в условиях динамичных экономических и социальных изменений в практике управления все в большей степени утверждается инновационный метод освоения социального пространства – его технологизация. В ходе развертывания научно-технической и информационной революций значительно усилилось внимание к социальным компонентам технологий и появилась возможность распространить технологический подход на все стороны общественной жизни: экономику, социальное управление, образование, воспитание, политику, право и др. Причем в каждой из них технологизация основывается не просто на обобщении эмпирического опыта, а на новейших достижениях современной науки и техники.

В современной техногенной цивилизации решающую роль играет постоянный поиск и применение новых технологий, причем не только производственных технологий, обеспечивающих экономический рост, но и технологий социального управления и социальных коммуникаций [1].

Ценности техногенной цивилизации легли и в основу теории и практики социальных технологий как специфических процедур преобразования социальной реальности. Л.Я. Дятченко подчеркивает: «Социальные технологии не имеют принципиальных отличий от технологий в сфере материального производства, поскольку возможность технологизировать любой социальный процесс заложена в структуре человеческой деятельности и в самой природе человека» [2].

Это и обуславливает необходимость технологизации судопроизводства.

Основная часть. Технологизация познавательных процедур и практических действий, направленных на достижение целей судопроизводства и оптимизация человеческих ресурсов позволяет повысить его эффективность и соответствовать современным реалиям. Результатом технологизации судопроизводства станет переход к цифровому судопроизводству, т.е. урегулированному нормами процессуального права деятельности суда, участвующих в деле лиц и других участников процесса, а также органов исполнения судебных решений по разрешению юридических дел. Здесь ключевым фактором являются данные в цифровом виде, обработка и использование результатов анализа которых по сравнению с традиционными формами судопроизводства позволяют существенно повысить его эффективность.

[10] На логистичность права указывает тот факт, что нормы, регламентирующие использование современных технологий, нашли свое место во всех его современных отраслях.

[11] Более подробно см., Бертовский Л.В. Высокотехнологичное право: понятие, генезис и перспективы. Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С. 735-749.

К основным направлениям развития цифрового судопроизводства можно отнести: нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и безопасность[12].

С этой точки зрения, представляется важным следующие процессы:

1. получение и трансформация релевантной для целей судопроизводства информации в машиночитаемую;
2. дальнейшее ее накопление;
3. анализ и обработка полученной информации;
4. формирование предлагаемого решения;
5. обратная трансформация информации в «человекочитаемый» вид;
6. использование полученных результатов.

В современном судопроизводстве наибольшее количество информации к правоприменительным органам поступает после соответствующей трансформации в виде документов, реже в натуральном виде (вещественные доказательства, похищенное или оспариваемое имущество и т.д.). К документам можно отнести различные заявления, справки, выписки, протоколы следственных действий и др. Для последующей обработки все они должны быть стандартизированы для преобразования их в машиночитаемую форму. В отношении документов больших проблем не возникает: сегодня успешно используются как технические средства сканирования, так и программные методы распознавания[13]. Хотя здесь имеются свои проблемы. Накопленные эмпирические данные в виде различных справок, обзоров, дел в архивах судов, следственных отделов содержаться на бумажных носителях. При этом данные материалы необходимы для последующего машинного анализа и использования, а также создания нейросетей для выработки предложений решений по аналогичным делам.

Они требуют соответствующей обработки, как это делается в современных библиотеках, для чего кадровое и техническое обеспечение в правоприменительных органах отсутствует. Материальные и временные затраты довольно существенные.

---

[12] Более подробно см., Бертовский Л.В. Технология блокчейн в уголовном процессе как элемент цифрового судопроизводства Проблемы экономики и юридической практики. 2017. № 1. С. 134/

[13] Оптическое распознавание символов (англ. optical character recognition, OCR) — механический или электронный перевод изображений рукописного, машинописного или печатного текста в текстовые данные, использующиеся для представления символов в компьютере (например, в текстовом редакторе). Распознавание широко применяется для преобразования книг и документов в электронный вид, для автоматизации систем учёта в бизнесе или для публикации текста на веб-странице. Оптическое распознавание символов позволяет редактировать текст, осуществлять поиск слов или фраз, хранить его в более компактной форме, демонстрировать или распечатывать материал, не теряя качества, анализировать информацию, а также применять к тексту электронный перевод, форматирование или преобразование в речь: https://ru.wikipedia.org/wiki/Оптическое_распознавание_символов

Организации, которые занимаются подобными вопросами, оценивают сканирование одного листа в 1 рубль и еще один рубль придется заплатить за его распознавание. С учетом объемов архивов сумма получается колоссальной! И это, не считая проблем с распознаванием рукописных текстов, для которых соответствующего программного обеспечения надлежащего качества пока нет, а те, которые есть дороги, и предъявляют высокие требования к аппаратному обеспечению.

В 2019 году виртуальный суд города Пекина начал рассматривать некоторые категории гражданских дел, где в качестве судьи председательствовал искусственный интеллект. Внешне это выглядит так, как будто реальный судья разбирает юридическое дело. Причем мимику, жесты и поведение скопировали с реального судьи. Китайские чиновники уверены, что за цифровыми помощниками будущее мирового правосудия. Как отметил по этому поводу Ни Дефэн, вице-президент интернет-суда в Ханчжоу: «Ведение дел на более высокой скорости – это и есть современное право, потому что задержка правосудия приравнивается к отказу в правосудии» [3]. Однако, для того чтобы запустить этот суд нашим китайским коллегам потребовалось 17 лет, чтобы насытить нейросеть релевантной информацией.

Еще сложнее приходится, когда возникает задача создания цифрового образа различных материальных объектов, в т.ч. и места происшествия. В настоящее время имеются 3D-сканеры, которые осуществляют сканирование небольших объектов, а также сканеры, которые сканируют здания, сооружения, помещения, однако, первые хоть и обеспечивают точность от 0.018 мм, что позволяет сканировать в т.ч. и выявленные следы рук, для последующей идентификации, но работают медленно и, как указано выше, только с небольшими объектами, а вторые хоть и работают с большими объектами и достаточно быстро, обеспечить необходимую точность не могут. Кроме того, формат отсканированных изображений не всегда согласуется со средами виртуального моделирования: 3Ds Max, Maya, Rhinoceros и др. Для решения задач судопроизводства нужно решить техническую задачу по созданию компактного, мобильного комплекса, обеспечивающего 3D-сканирование больших объектов, таких как место происшествия, зданий, сооружений и др., с разрешением, позволяющем фиксировать различные следы, для проведение экспертных исследований, в т.ч. с целью последующего их воспроизводства (создания моделей, слепков и т.д.).

Таким образом, полученная в машиночитаемом виде информация готова к дальнейшему накоплению и обработке искусственным интеллектом (далее – ИИ). Дело в том, что для подготовки предложений по разрешению находящего в производстве дела может понадобиться дополнительная информация, которая может быть получена в результате производства следственных и судебных действий, а также

при обращении ИИ к различным организациям, базам данных (о судимости, административной практики, расписания движения транспортных средств и др.). Причем в последнем случае возникает проблема с обеспечения доступа к этим базам, а по большому счету мы здесь вплотную подходим к правосубъектности ИИ, которая должна решаться путем принятия соответствующих нормативных актов. Кроме того, представляется, что процессы получения, накопления и обработки информации должны осуществляться на основе проведенной унификации процессуальных действий для получения доказательств различных видах судопроизводства.

Считаю, что по результатам машинного анализа имеющейся информации ИИ должен готовить не решение по юридическому делу, а именно проект решения. Исследователи многих стран обсуждают проблему, может ли ИИ выступать в качестве судьи. Однако, многочисленные дискуссии пока ни к чему не привели, но все настойчивее звучат мнения о том, что судья имеет право на усмотрение и определенную свободу действий при принятие решении по делу, исходя из конкретной ситуации и своего внутреннего убеждения.

Так, в Европейской этической хартии об использовании искусственного интеллекта в судебных системах и окружающих их реалиях, которая принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3-4 декабря 2018 года), сформулировано пять принципов об использовании искусственного интеллекта в судебных системах и окружающих их реалиях:

1. уважения основополагающих прав: обеспечить разработку и внедрение инструментов и услуг, основанных на искусственном интеллекте, соответствующих основным правам;

2. недискриминации: определенным образом препятствовать развитию или усилению любой дискриминации между отдельными лицами или группами лиц;

3. качества и безопасности: при обработке судебных решений и данных, необходимо использовать сертифицированные источники и нематериальные данные с применением моделей, разработанных на междисциплинарной основе, в безопасной технологической среде;

4. прозрачности, беспристрастности и достоверности: сделать методы обработки данных доступными и понятными, разрешить проведение внешнего аудита;

5. контроля пользователем: избежать предписывающего подхода и позволить пользователю выступать в роли информированного лица, ответственного за свой выбор [4].

Наиболее важным представляется принцип контроля пользователя, в соответствии с которым, судья человек должен иметь возможность опровергнуть предложение искусственного интеллекта и принять собственное решение по делу, а участники процесса должны

иметь возможность прямого обращение к человеческому суду (состоящего из людей) и оспорить решение, принятое искусственным интеллектом.

Примечательно, что большинство споров среди специалистов ведется по поводу назначения наказания человеку, т.е. по сути принятия решения машиной, учету мотива совершенного поступка, при наличии смягчающих обстоятельств, в т.ч. и основанных на эмоциональном состоянии виновного. Но не менее важно понимать, как на основе какого алгоритма, принимается такое решение.

Поэтому «человекочитаемый» проект решения должен содержать ссылку на те факторы, которые позволили ИИ сделать те или иные выводы для окончательной оценки и принятия решения человеком.

Для качественного обеспечения функционирования цифрового судопроизводства непростой проблемой является низкий уровень технической подготовленности кадров. Это обуславливает значимость повсеместного введения и распространения дополнительного профессионального обучения современным информационным технологиям для всех категорий юристов [5]. Речь идет как о продвинутых пользователях офисных программ, так и о лицах, из числа обычных пользователей. При этом нередким является то, что даже в тех случаях, когда все-таки особенности современных IT-процессов находят свое отражение в учебных планах и содержании учебных дисциплин, их объем недостаточен, а их реализация в образовательном процессе зачастую формальна. Тогда как на Западе, зачастую, юристы, особенно работающие в сфере IT, имеют два полноценных образования – юридическое и техническое.

Для решения проблемы необходимо комплексно пересмотреть подходы к организации образовательного процесса, к видам и содержанию образовательных программ – на предмет все большего внедрения информационных и цифровых технологий [6], а также разработки новых инновационных профессиональных образовательных программ. Речь идет об образовательных программах как высшего, так и дополнительного образования, которые бы представляли собой интегрированный вариант двух самостоятельных направлений в образовательной деятельности – юридического и технического. При этом важно, чтобы данные программы реализовывались многопрофильными образовательными учреждениями образовательных учреждений высшего и дополнительного образования [7].

Данный подход был реализован в Институте высокотехнологичного права и социально-гуманитарных наук Национального исследовательского университета «Московский институт электронной техники» (далее – НИУ МИЭТ), где в настоящее время проводится подготовка студентов очной формы обучения (специалитет) по направлению подготовки 40.05.01 «Правовое обеспечение

национальной безопасности». Особенностью данного направления является наличие в учебном плане кроме традиционных дисциплин юридического цикла (уголовное право, уголовный процесс, гражданское право, гражданский процесс, криминалистика и т.д.), технических дисциплин: информатика и информационные технологии в профессиональной деятельности, основы языка Java, объектно-ориентированное программирование, гибридное моделирование, управление программными проектами, сети и коммуникации, базы данных, интернет программирование, нейронные сети, интерактивные графические системы и другие. При этом юридические дисциплины составляют 60 процентов учебного плана, технические – 40 процентов. Обучение осуществляют опытные специалисты, имеющие научные степени кандидатов и докторов наук. Возможность осуществления данной программы обусловлена наличием уникальной суперсовременной технической базы НИУ МИЭТ, позволяющей приобретать обучающимися практических навыков в использовании высоких технологий. Объединение юридических и технических знаний даст возможность выпускникам активно участвовать в процессах цифровизации, внедрения искусственного интеллекта, технологии блокчейн в государственные институты, совершенствования нормативной правовой базы. Такая программа осуществляется в Российской Федерации впервые.

Очевидно, что рассматриваемый подход к организации судопроизводства потребует внесения значительных корректив в реализуемую Концепцию судебной реформы, а также в целый ряд нормативных правовых актов: УПК РФ, ГПК РФ, АПК РФ, «О судебной системе Российской Федерации», «О прокуратуре Российской Федерации» и ряд других. Кроме того, необходима разработка соответствующих планов мероприятий («дорожных карт»), сформированных в рамках системы управления реализацией вышеуказанного указа Президента РФ от 09.05.2017г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы».

При этом следует отметить, что в Республике Казахстан очень хорошими темпами ведется актуализация нормативной базы, и в этом плане, в ряде случаев, превосходят интенсивность законодательной деятельности в Российской Федерации. Об этом свидетельствует принятие и реализация целого ряда нормативных актов, таких как: Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК, Закон РК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам усиления защиты права собственности, арбитража, оптимизации судебной нагрузки и дальнейшей гуманизации уголовного законодательства» от 21 января 2019 года № 217-VI ЗРК, «О внесении изменений и дополнений в

Гражданский процессуальный кодекс Республики Казахстан по вопросам внедрения современных форматов работы судов, сокращения излишних судебных процедур и издержек» от 10 июня 2020 года № 342-VI ЗРК, Постановление Правительства Республики Казахстан от 12 декабря 2017 года №827 «Об утверждении Государственной программы «Цифровой Казахстан» и целый ряд других, реализованы проекты «Е-суд» и «Виртуальный суд».

В заключении необходимо отметить, что создание цифрового судопроизводства в настоящее время продвигается медленными темпами. Сказывается и инертность некоторых руководителей, отсутствие достаточного финансирования и многое другое. Работа по технологизации судопроизводства потребует больших кадровых, материальных, временных и иных ресурсов, но альтернативные пути, по которому сейчас продвигается юридическое сообщество, нет, и чем раньше, и активней будет осуществляться эта деятельность, тем эффективней будет результат.

Список использованных источников:

1. Понятие технологизации [Электронный ресурс] - Режим доступа: https://helpiks.org/8-97788.html (дата обращения 15.04.2023).

2. Дятченко Л.Я. Социальные технологии в управлении общественными процессами. - М.: Белгород: Центр социальных технологий, 1993. - С. 4.

3. Семь смертных грехов искусственного интеллекта [Электронный ресурс] - Режим доступа: https://trends.rbc.ru/trends/social/5eb299089a79476e9fd77f5c (дата обращения: 14.04.2023).

4. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях Принята на 31-м пленарном заседании ЕКЭП (Страсбург, 3-4 декабря 2018 года) [Электронный ресурс] - Режим доступа: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4.

5. Курбатова С.М., Айснер Л.Ю., Наумкина В.В. К вопросу о проблематике качества высшего образования по направлению подготовки «юриспруденция» // Современный ученый. 2020. № 6. С. 145-151.

6. Трашкова С.М., Айснер Л.Ю. Комплементация информационных технологий и системы образования сквозь призму российского законодательства // Научное обозрение: гуманитарные исследования. 2017. № 8-9. С. 9-11.

7. Бертовский Л.В. Технология блокчейна в уголовном процессе как элемент цифрового судопроизводства // Проблемы экономики и юридической практики. 2017. № 6. С. 226-230.

УДК 343.140.02:004

Воскобитова Лидия Алексеевна
Заведующий кафедрой уголовно-процессуального права Московского государственного юридического университета имени О.Е. Кутафина, доктор юридических наук, профессор,
г. Москва, Российская Федерация

ТРАНСФОРМАЦИЯ ДОКАЗЫВАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Аннотация. В статье рассматриваются современные изменения уголовного судопроизводства, связанные с использованием цифровых технологий в доказывании по уголовным делам; трансформация теоретических представлении о доказательстве и доказывании, необходимость уточнения процессуального регулирования процесса доказывания, обеспечение своевременного обнаружения и интерпретации цифровой информации, процесса преобразования ее в доказательство, необходимость трансформации процессуального статуса специалиста и переводчика.
Ключевые слова: уголовное судопроизводство; доказывание; доказательство; цифровая информация; обнаружение; получение; преобразование в процессуальное доказательство.

Аннотация. Мақалада қылмыстық істерді дәлелдеуде цифрлық технологияларды қолдануға байланысты қылмыстық сот ісін жүргізудің заманауи өзгерістері қарастырылады; дәлелдеу және дәлелдеу туралы теориялық түсініктерді өзгерту, дәлелдеу процесін процестік реттеуді нақтылау қажеттілігі, цифрлық ақпаратты уақтылы анықтау мен түсіндіруді қамтамасыз ету, оны дәлелдеуге айналдыру процесі, маман мен аудармашының іс жүргізу мәртебесін өзгерту қажеттілігі.
Түйінді сөздер: қылмыстық сот ісін жүргізу; дәлелдеу; дәлелдеу; сандық ақпарат; анықтау; алу; процестік дәлелдемесіне айналдыру.

Annotation. The article discusses modern changes in criminal proceedings related to the use of digital technologies in proving criminal cases; the transformation of theoretical concepts of proof and proof, the need to clarify the procedural regulation of the process of proof, ensuring timely detection and interpretation of digital information, the process of converting it into evidence, the need to transform the procedural status of a specialist and translator.
Keywords: criminal proceedings; proof; proof; digital information; detection; receipt; transformation into procedural evidence.

Введение. Доказывание в уголовном судопроизводстве строится на ряде констант, обусловленных самой природой данной деятельности. Эти константы формировались на протяжении истории развития уголовного судопроизводства и имеют место в современном уголовном процессе разных стран и разных исторических типов. К их числу следует отнести тесную *связь уголовного судопроизводства с уголовных правом* в силу того, что судопроизводство является единственной

легальной формой применения норм уголовного права к единичному уголовному правонарушению. *Правоприменительный характер*, как другая константа уголовного судопроизводства, требует по каждому уголовному делу сначала установить *фактическую основу* совершенного уголовного правонарушения: познать, что фактически произошло в реальной жизненной ситуации, кто это совершил, есть ли вина и каковы ее формы, т.е. познать все юридически значимые фактические обстоятельства, позволяющие правильно применить нормы уголовного права. Для этого требуется особая процессуально-правовая технология познавательной деятельности, чтобы правильно установить фактическое проявление всех признаков конкретного состава преступления в частном случае совершения правонарушения, а также всех процессуально значимых фактических обстоятельств (времени, места, обстановки, ситуации, результатов и пр.).

Познавательная деятельность в уголовном судопроизводстве начинается с момента обнаружения преступления и сопровождает всю дальнейшую процессуальную деятельность в отношении конкретного лица. Для ее осуществления вовлекаются и иные заинтересованные субъекты, чье право нарушено преступлением. Также возникает необходимость взаимодействовать с иными лицами, привлекаемыми в качестве свидетелей, понятых, специалистов, экспертов, переводчиков и т.д. Еще одной константой является *требование правильности и достоверности,* предъявляемое к процессуальному познанию. Познающие субъекты процесса не имеют права на ошибку: привлечение к ответственности невиновного, привлечение не за то преступление, которое было совершено, без учета тяжести преступления и личности виновного является незаконным во всех правопорядках. И, наконец, *презумпция невиновности, как* константа уголовного судопроизводства, требует своего опровержения посредством *доказанности* всех фактических обстоятельств дела вне разумных сомнений. Это предполагает проверку и познание не только обвинительных, но и оправдательных; не только уличающих, но и оправдывающих обстоятельств и аспектов совершенного деяния.

Поскольку уголовное судопроизводство это деятельность, осуществляемая при взаимодействии людей, она прежде всего вырабатывает *социальные технологии* и формирует определенный набор методов, средств, приемов такого взаимодействия, обеспечивая достижение целей данной деятельности. Социальная технология формируется в зависимости от целей судопроизводства, поэтому технология инквизиционного процессуального познания существенно отличается от технологии современного. В современном процессе различаются технологии познания, например, в англо-саксонском уголовном процессе, строящемся на теории уголовного иска, и континентальном, строящемся на принципе публичности. Наиболее

успешные социальные технологии познания получают процессуально-правовое регулирование и становятся нормами доказательственного права. Эти правовые предписания превращают социальную технологию в *процессуально-правовую*, придавая легальность результатам познания и в известной мере обеспечивая правильность познания. Появление *цифровых технологий* и их тотальное проникновение в сферу социальных отношений не может не затронуть право в целом и уголовно-процессуальное познание и доказывание, в частности.

Основная часть. Вторжение цифровых технологий в уголовное судопроизводство не ждет специального разрешения законодателя и фактически, хотя и фрагментарно, уже присутствует в нем. Цифровые технологии существенно меняют делопроизводство, облегчая работу с процессуальными документами и возможности оперативной связи между различными субъектами процесса. Электронные базы данных позволяют получать информацию, имеющую юридическое значение при производстве по делу. Использование цифровых устройств при проведении следственных действий, например, видеозаписи, фотографирования, получения локализации нахождения средств связи и пр. позволяет получать информацию, во-первых, быстрее, во-вторых, с большей точностью, в третьих, с возможность более детального ее изучения (качество изображений, возможность их увеличения, фиксации более мелких деталей). Как эти технологии влияют на процессуальное доказывание? По мнению Л.В. Головко, цифровизация уголовного судопроизводства может быть сопоставлена с общим техническим развитием: гусиное перо, которым писались процессуальные документы в 18-19 веке, было успешно заменено пишущими машинками в веке 20-м, а теперь последние заменяются компьютерами, но это не меняет обозначенные выше константы процессуального познания и доказывания. Увы, это не так. Цифровые технологии проникают значительно глубже и требуют весьма серьезного изучения и прогноза возможных и необходимых трансформаций процессуального познания и доказывания как на уровне теоретических представлений, так и на уровне процессуального регулирования[14]. На данный момент такие трансформации уже проявляют себя в силу того, что сама преступная деятельность также проходит свою «цифровизацию». Появляются новые *методы совершения* преступлений, давно известных уголовному законодательству. Использование цифровых технологий преступниками требует новых навыков, правил, специальных знаний как для их выявления, так и для их расследования, раскрытия, получения

[14] Не случайно на уровне международных актов уже делаются попытки определить границы допустимости цифровизации судопроизводства. См.: Руководящие принципы Комитета министров Совета Европы в отношении электронных доказательств в гражданском и административном производстве: приняты Комитетом министров 30 января 2019 г., на 1335-м заседании заместителей министров // URL: https://www.coe.int/ru/web/portal/-/committeeof-ministers-adopts-guidelines-on-electronic-evidence-in-civil-and-administrative-proceedin-1.

достаточных и достоверных доказательств для их судебного разрешения[15].

Например, использование цифровых технологий при совершении мошенничества и похищениях таким способом денежных средств со счета потерпевшего[16] или незаконный оборот наркотических и иных запрещенных веществ без контакта покупателя и продавца, через социальные сети. Эти и многие иные преступления, которые совершаются в физическом мире, оставляют следы. Выявление таких следов и их процессуальное закрепление позволяет получать привычные доказательства, хотя расследование таких преступлений сопровождается необходимостью учитывать особенности цифровых технологий. Например, при расследовании дел о незаконном обороте наркотиков следователь, традиционно, проводит осмотр места «закладки товара» и действует по правилам осмотра места происшествия, фиксируя различного рода «физические» следы: общий вид места, окружающую среду, возможные следы обуви, отпечатков пальцев или иные микро следы, оставляемые и преступником, сделавшим эту «закладку», и «покупателем», приходившим забрать ее. Следователь будет производить и допросы фигурантов дела, возможных свидетелей; проводить экспертизы и пр.

Однако существенную роль в расследовании таких преступлений начинают играть цифровые технологии. Например, анализ соцсетей помогает выявлять и адреса, с которых предлагается такого рода «товар», и поступающий запрос на приобретение такого «товара». Наличие цифровых видеокамер позволяет отследить и выявить лиц, которые находились в районе «закладки-покупки». Цифровые системы проведения платежей позволяют выявлять счета, криптокошельки, иные формы цифровых расчетных операций конкретных лиц и устанавливать как продавца, так и покупателя в этих незаконных операциях. Существенную роль в раскрытии разного рода преступлений играют различного рода видеокамеры, размещенные на улицах города, в общественных местах, торговых точках, в подъездах жилых домов[17].

---

[15] Этим вопросам уделяется внимание и в зарубежных исследованиях, например см.: Маршалл, Ангус М, Цифровая экспертиза: Цифровые доказательства при расследовании уголовных дел. Чичестер, Великобритания: Вайли-Блэквелл. 2008. электронная книга. ISBN: 9780470517758 и др.

[16] Например, совершение мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ) или мошенничества в сфере компьютерной информации (ст.159.6 УК РФ).

[17] Иккерт А. В. К вопросу о современном состоянии законодательства в сфере использования технических средств фиксации административных правонарушений в области дорожного движения // Актуальные вопросы юридической науки. 2019. № 4 (4). С. 35. Например, в Москве есть программа «Безопасный город», благодаря которой установленные камеры видеонаблюдения позволяет раскрывать до 70% преступлений, среди которых совершаемые ДТП, кражи, разбойные нападения, драки, хулиганство. Записи с камер видеонаблюдения может запросить не только следователь, но и любой человек, в том числе потерпевший, у которого, например, угнали или повредили автомобиль; адвокат,

Такого рода видеозаписи оформляются и изымаются; осматриваются и приобщаются к делу в порядке ст.81 УПК РФ. Суд исследует их в совокупности со всеми иными доказательствами и учитывает при принятии решения по делу. Следует признать, такого рода видеозаписи нередко дают более точную информацию, чем, например, свидетельские показания. Они позволяют уточнять и детализировать обстоятельства преступного правонарушения, но нередко такие технические источники информации позволяют установить и невиновность лица, привлекаемого к ответственности. Цифровая видеозапись позволяет следователю создавать цифровую модель происшествия, чтобы понять, например, можно ли было избежать столкновения в данном дорожно-транспортном происшествии (ДТП), кто из водителей и как нарушил правила. Можно констатировать, что в расследовании преступлений, которые совершаются в физическом мире, цифровая техника дает значительно больше возможностей для более точного познания и доказывания фактических обстоятельств преступления.

Трансформация регулирования доказывания по таким уголовным делам будет происходить путем уточнения процессуального порядка использования различных видов цифровой техники, получения и хранения цифровой информации. Однако понятие доказательства в этих ситуациях сохраняет свою природу *следа,* оставленного преступлением в объективной реальности, и свою информационную природу как *фактических* данных, имеющих значение для производства по данному делу[18] (ст.674 УК РФ и ст.111 УПК РК). Сохранится и требование к достаточности доказательств, потому что цифровое доказательство должно находить подтверждение в остальных доказательствах, собранных по делу, в совокупности своей позволяя следователю, государственному обвинителю и суду сформировать в своем сознании непротиворечивый и полный образ совершенного преступления как фактическую основу для отыскания и применения адекватной уголовно-правовой нормы.

Принципиально иная ситуация доказывания возникает при совершении преступлений, порожденных самим процессом цифровизации: это так называемые «компьютерные» преступления[19]. Развитие уголовного права уже выделяет новые виды преступлений, совершаемых исключительно посредством цифровой техники и в цифровой среде. В УК РФ, например, появилась глава 28 «Преступления в сфере компьютерной информации», куда вошли такие

который участвует в деле в качестве защитника или представляет интересы потерпевшего. См. сайт: URL:https://www.mos.ru/drbez/dokuments/programma-besopasnyi-gorod/view/215646220

[18] *Шейфер С. А.* Доказательства и доказывание по уголовным делам: Проблемы теории и правового регулирования. М.: Норма, 2009

[19] Более подробно об этом см. П.С. Пастухов. Основы теории электронных доказательств. Монография /под ред. С.В. Зуева. -М.: Юрлитинформ. 2019. С. 31-62

преступления, как «Неправомерный доступ к компьютерной информации» (ст.272); «Создание, использование и распространение вредоносных компьютерных программ» (ст. 273) и др. подобные. В УК РК также выделена глава **7** «Уголовные правонарушения в сфере информатизации и связи», включающая, например «Неправомерные уничтожение или модификация информации» (ст.205 УК РК); «Нарушение работы информационной системы или сетей телекоммуникаций» (ст.207 УК РК); «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов» (ст.210 УК РК) и некоторые другие.

Если обычные преступления совершаются в социальной среде и проявляют себя так или иначе в форме жизненного события, то компьютерные преступления совершаются в цифровой среде, в которой выделяются три уровня информационных отношений: *технический* (сетевой), *программн*ый (сервисный) и *информационный* (собственно информация, присутствующая в сети)[20] Для компьютерных преступлений характерно то, что: а) они *не существуют вне цифровой среды*, поскольку их нет в реальном мире, значит нет и привычных для нас «аналоговых» следов, типа: удар-повреждение; б) они *осуществляются в мире цифровой информации*, но способны захватывать любой из указанных выше уровней: *технический*, повреждая компьютер или в целом сеть; *программный,* нарушая, искажая, уничтожая программу, или *информационный*, искажая, блокируя циркулирующую информацию, создавая ложную информацию; в) они выражены *цифровым языком*, поэтому требуют *не перевода* с цифрового на разговорный язык, а *специальной интерпретации-объяснения* значения, смысла, действия и последствий цифрового знака или цифровой записи; г) они и информация о них *не существуют вне цифрового носителя*, поэтому если уничтожается носитель, уничтожается и информация и само существование преступления.[21] И эта ситуация требует существенной трансформации практически всех представлений о доказывании в уголовном судопроизводстве: иного определения предмета доказывания; понимания, что доказательство – это не только фактические, но еще и цифровые данные, требующие собственного процессуального порядка их обнаружения, собирания и использования; что следственные действия по их собиранию, проверке и оценке

[20] Бачило И.Л., Лопатин В.Н., Федотов М. А. Информационное право: учебник / под ред. акад. РАН Б. Н. Топорнина. Санкт-Петербург: Юридический центр Пресс, 2001. С. 663; Ю.В. Волков, Уровневое регулирование цифровых отношений / Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под : ред. И.Р. Бегишева, Е.А. Громовой, М.В. Залоило, И.А. Филиповой, А.А. Шутовой. В 6 т. Т. 1. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. С.81-86

[21] Основы теории электронных доказательств: монография /под ред. С.В. Зуева. -М.: Юрлитинформ. 2019, С.25-26, 28, 30

невозможны без специалиста по цифровым технологиям во взаимодействии со следователем и иными участниками процесса на всех этапах работы с цифровой информацией и, очевидно, другие уточнения и теоретических представлений, и правового регулирования.

Заключение. Прежде всего требуется трансформация существующих уголовно-правовых представлений о признаках каждого их составов компьютерного преступления, только после этого можно будет формулировать предмет доказывания по таким делам. Представляется, что для применения нормы уголовного права в этих случаях, как минимум, потребуется устанавливать, на каком из цифровых адресов произошел несанкционированный сбой и в чем он выразился: в повреждении технической аппаратуры, или программы, или вторжении в информацию. Возможно, это позволит предположить, что могло иметь место преступное вторжение. Далее возможно технически удастся проследить, с какого адреса пришла вредоносная программа или информация. И только через сопоставление технических (сетевых) манипуляций может быть будет установлен и субъект этого преступления. Это усложняет задачи и проблемы доказывания. Во-первых, преступление совершается вне реального мира, не очевидно для всех кроме преступника, следовательно, его трудно выявлять обычными способами. Во-вторых, оно не оставляет того, что можно было бы идентифицировать как след, который можно изъять, зафиксировать, приобщить к материалам дела. Возможно, информация, выраженная языком цифрового кода или алгоритма, будет понята специалистом как свидетельствующая о намеренном вредоносном действии с точки зрения техники или технологии. Однако это еще не свидетельствует о преступности совершенного деяния, ибо язык цифр требует преобразования в человеческий, единственный, на котором можно описать признаки состава преступления. Сейчас много внимания уделяется проблеме создания машиночитаемого права[22]. Эта проблема уже достаточно успешно решается. Но вот обратной логической операции, когда машина могла бы сказать человеку, что то или иное цифровое действие является преступным, пока еще нет. В уголовном судопроизводстве есть два субъекта, которые предназначены для оказания содействия следователю и суду: специалист, который привлекается, когда возникает необходимость в использовании неких специальных знаний для оказания содействия следователю (ч.1 ст.58, ч.2.1 ст.82 УПК РФ), и переводчик, который призван переводить текст с одного языка на другой (ч.1 ст.59 и ч.2 ст. 169 УПК РФ).

Однако в настоящее время их правовое положение не пригодно для выявления и расследования компьютерного преступления.

[22] Хабриева Т. Я., Черногор Н. Н. Будущее права. Наследие академика В. С. Степина и юридическая наука. Москва: ИНФРА-М, 2020; Бертовский Л.В. Высокотехнологичное право: понятие, генезис и перспективы. Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С. 735—749 и др.

Специалист действует только в рамках задач, поставленных следователем, но следователь не может знать, посредством каких знаков, кодов, символов может проявить себя вредоносный характер цифрового действия, поэтому он не сможет конкретизировать задачу. Одновременно специалист, не знающий признаков данного состава преступления, не знает, а что в воспринимаемой им цифровой (кодовой) информации, собственно, необходимо следователю ввиду того, что будет иметь правовое значение. Переводчик также не приспособлен к такой ситуации. Цифровой язык не создан для свободного социального взаимодействия людей. Он создан для взаимодействия «человек-машина» и человек создает нечто искусственное, формально алгоритмичное для передачи команд машине и получения ее реакции. Чтобы выявить правовые смыслы в таком взаимодействии необходим не переводчик, а *интерпретатор.* Он должен понимать смысл и назначение каждой цифровой команды-кода; знать, какую реакцию машины это порождает; уметь объяснить человеческим языком весь процесс взаимодействия «человек-машина-человек». Поэтому трансформация доказывания по уголовным делам о компьютерных преступления необходима и неизбежна, однако она требует профессионального взаимодействия и совместных исследований юристов со специалистами в области цифровых технологий.

Список использованных источников:

1. Руководящие принципы Комитета министров Совета Европы в отношении электронных доказательств в гражданском и административном производстве: приняты Комитетом министров 30 января 2019 г., на 1335-м заседании заместителей министров // URL: https://www.coe.int/ru/web/portal/-/committeeof-ministers-adopts-guidelines-on-electronic-evidence-in-civil-and-administrative-proceedin-1
2. Маршалл, Ангус М, Цифровая экспертиза: Цифровые доказательства при расследовании уголовных дел. Чичестер, Великобритания: Вайли-Блэквелл. 2008. электронная книга. ISBN: 9780470517758 и др.
3. Уголовный кодекс Российской Федерации /СПС Консультант Плюс
4. Уголовный кодекс Республики Казахстан /СПС Консультант Плюс
5. Уголовно-процессуальный кодекс Российской Федерации /СПС Консультант Плюс
6. Уголовно-процессуальный кодекс Республики Казахстан /СПС Консультант Плюс
7. Иккерт А.В. К вопросу о современном состоянии законодательства в сфере использования технических средств фиксации административных правонарушений в области дорожного движения // Актуальные вопросы юридической науки. 2019. № 4 (4). С. 35.
8. Сайт: URL:https://www.mos.ru/drbez/dokuments/programma-besopasnyi-gorod/view/215646220
9. Шейфер С.А. Доказательства и доказывание по уголовным делам: Проблемы теории и правового регулирования. М.: Норма, 2009
10. Основы теории электронных доказательств. Монография /под ред. С.В. Зуева. -М.: Юрлитинформ. 2019. С..25-26, 28, 30; 31-62;

11. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник / под ред. акад. РАН Б. Н. Топорнина. Санкт-Петербург: Юридический центр Пресс, 2001. С. 663

12. Ю.В. Волков, Уровневое регулирование цифровых отношений / Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под: ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 1. – Казань: Изд-во «Познание» Казанского инновационного университета, 2022. С.81-86

13. Хабриева Т.Я., Черногор Н.Н. Будущее права. Наследие академика В. С. Степина и юридическая наука. Москва: ИНФРА-М, 2020;

14. Бертовский Л.В. Высокотехнологичное право: понятие, генезис и перспективы. Вестник РУДН. Серия: Юридические науки. 2021. Т. 25. № 4. С. 735—749 и др.

004.8:343.98

Гармаев Юрий Петрович
Директор Центра правового и антикоррупционного просвещения,
профессор кафедры уголовного права, процесса и криминалистики
Бурятского государственного университета имени Доржи Банзарова,
доктор юридических наук, профессор,
старший советник юстиции (в отставке),
г. Улан-Удэ, Российская Федерация

ЦИФРОВИЗАЦИЯ И ИННОВАЦИОННЫЕ ПОДХОДЫ В ОБУЧЕНИИ СЛЕДОВАТЕЛЕЙ КРИМИНАЛИСТИКЕ

Аннотация. Цель работы предложить общие и частные инновационные средства и методы обучения действующих и будущих следователей, их мотивации к профессиональной подготовке. Анализируются особенности и недостатки организации современной следственной деятельности, а также отдельные аспекты обучения молодежи; проблемы соответствующих научных прикладных разработок. На основе этого анализа сформулированы предложения: о приоритете аудио-видеоконтента, геймификации в обучении, разработки компьютерных игр, специализированных компьютерных программ и мобильных приложений, иных обучающих электронных ресурсов. Важно готовить следователей к необходимости постоянного обучения, гибкой адаптации к меняющимся условиям цифровизации. А главное – постоянно мотивировать их к повышению квалификации в интересной и творческой профессии.

Ключевые слова: цифровизация уголовного судопроизводства; недостатки расследования; инновационные методы обучения следователей; криминалистическая тактика; криминалистическая методика; компьютерные игры в криминалистике.

Аннотация. Жұмыстың мақсаты қазіргі және болашақ тергеушілерді оқытудың жалпы және жеке инновациялық құралдары мен әдістерін ұсыну, олардың кәсіби дайындыққа мотивациясын беру. Қазіргі заманғы жедел-іздестіру қызметін ұйымдастырудың ерекшеліктері мен кемшіліктері, сондай-ақ жастар тәрбиесінің жекелеген аспектілері талданады; сәйкес ғылыми қолданбалы әзірлемелердің мәселелері. Осы талдаудың негізінде аудио-бейне контенттің басымдығы, білім берудегі геймификация, компьютерлік ойындарды, мамандандырылған компьютерлік бағдарламалар мен мобильді қосымшаларды және басқа да білім беру электрондық ресурстарын дамыту бойынша ұсыныстар тұжырымдалды. Тергеушілерді үздіксіз оқыту қажеттілігіне, цифрландырудың өзгермелі жағдайларына икемді бейімделуіне дайындау маңызды. Ең бастысы, оларды қызықты және шығармашылық мамандықта біліктілігін арттыруға үнемі ынталандыру.

Түйінді сөздер: қылмыстық процесті цифрландыру; тергеудегі кемшіліктер; тергеушілерді оқытудың инновациялық әдістері; криминалистикалық тактика; криминалистикалық техника; криминалистикадағы компьютерлік ойындар.

Annotation. The purpose of the work is to offer general and particular innovative means and methods for teaching current and future investigators, their motivation for professional training. The features and shortcomings of the organization of modern

investigative activities, as well as certain aspects of youth education are analyzed; problems of relevant scientific applied developments. Based on this analysis, proposals were formulated: on the priority of audio-video content, gamification in education, the development of computer games, specialized computer programs and mobile applications, and other educational electronic resources. It is important to prepare investigators for the need for continuous training, flexible adaptation to the changing conditions of digitalization. And most importantly, constantly motivate them to improve their skills in an interesting and creative profession.

Keywords: digitalization of criminal proceedings; shortcomings of the investigation; innovative methods of training investigators; forensic tactics; forensic technique; computer games in criminalistics.

Уголовно-процессуальная, криминалистическая деятельность стремительно меняются в условиях глобальной цифровизации. Россия, как и Казахстан, активно вовлечен в трансформационные процессы. Изучение казахстанского опыта ведения электронного документооборота и возможности расследования уголовных дел, условно говоря, в «электронном» формате [1] указывает на значимые успехи в этой области, заслуживающие пристального внимания.

В России также реализуется множество проектов, связанных с цифровизацией. В частности, Национальная программа «Цифровая экономика Российской Федерации» включает формирование правовой основы обеспечения допустимости электронных доказательств [2].

Как отмечается в современных публикациях, дальнейшее проникновение современных информационных технологий в уголовное судопроизводство, в совокупности с ясно осознаваемой потребностью его модернизации, а также с учетом компьютеризации преступной деятельности не могут не ставить ряда обоснованных вопросов [3].

Соответственно возникает необходимость актуализации криминалистического научного и учебно-методического обеспечения работы следователя в новой цифровой реальности. Можно ли сказать, что науки, а за ними и учебные дисциплины антикриминального цикла, прежде всего, криминалистика, готовы к неизбежной трансформации? Думается, что не в полной мере.

Ни для кого не секрет, что в адрес этих наук уже давно приходят критические замечания, связанные с их отставанием от потребностей практики [4]. «В России, как и в некоторых других государствах, наблюдается излишняя теоретизированность юридических научных исследований, и практики в этом неоднократно совершенно справедливо упрекали теоретиков… Можно сказать, что наука существует ради науки» [5]. Львиная доля всех публикаций в криминалистике – это многостраничные печатные издания, либо они же, но просто переведенные в электронный текст (форматы Word, PDF и т.п.) Содержание этих изданий – сложные для восприятия и многословные тексты. Мягко говоря, далеко не во всех юридических вузах и учреждениях по повышению квалификации криминалистическая

(как и любая иная) дидактика адаптирована к вызовам цифровизации. В результате, хотя и далеко не только поэтому, качество подготовки следователей, их адаптивность к новым реалиям оставляют желать много лучшего.

А теперь посмотрим, кто он такой – современный следователь как обучающийся? Современные подростки и молодежь, взрослые люди возраста 25-55 лет – то есть, в том числе, будущие и действующие следователи, в настоящее время значительно больше, чем книгами, пользуются стационарными и мобильными компьютерами (ноутбуками, планшетами и др.) для серфинга в Интернете, социальных сетях, мессенджерах и т.п. как на работе, так и дома, а также в общественном транспорте, иных поездках. Граждане ежедневно используют смартфоны и иную сложную мобильную технику на операционных системах «iOS», «Android», реже «Windows mobile», на которых установлено современное программное обеспечение, позволяющее в любом месте читать и слушать книги, просматривать фото, презентации и слайд-шоу, видео и прочий контент.

Исследования показывают, что современный человек уже больше визуал и аудиал, нежели кинестетик. Видео-аудио, игровой контент давно побеждает текстовый формат в борьбе за внимание аудитории. Может ли наука криминалистика, криминалисты игнорировать столь яркие, тотальные изменения в характеристике своей основной целевой аудитории? Думается, что нет. Есть ли смысл пенять на то, что «… были люди в наше время, не то, что нынешнее племя: богатыри – не вы!...» [6] и настойчиво требовать от следователей того, к чему большинство не очень склонно? А если не выполняют, то: «… что ж, мы умываем руки…» и продолжать корить «племя молодое, незнакомое»? Думается, что, конечно же, нет. Безусловно, просветительская работа, обучение и повышение квалификации действующих и будущих следователей, их общественных помощников, наша – ученых и преподавателей вузов, необходимая и обязательная задача, и даже миссия. Стимулировать их к изучению печатной литературы – нашего пока еще основного научного результата, это, разумеется, необходимо и неизбежно. Но все же следует признать и то, что наука также должна подстраиваться под нужды современного, если так можно выразиться, среднестатистического следователя.

Многолетние авторские исследования, включая опросы респондентов-следователей, сотни проведенных занятий по повышению квалификации сотрудников следственных подразделений и иных правоохранительных органов, позволяют сделать неутешительные выводы. Большинство следователей не изучают регулярно криминалистическую научную, включая даже прикладную литературу, пособия и учебники.

Аналогичные данные подтверждаются иными исследователями. В.Н. Карагодин, будучи деканом факультета повышения квалификации (с дислокацией в г. Екатеринбурге) Академии Следственного комитета России, заявляет о слабой востребованности на практике работ ученых-криминалистов. Причиной автор, кроме прочего, называет перегруженность текстов теоретическими положениями. Около 50 % опрошенных им следователей сообщили, что по этой причине не знакомятся регулярно с литературой по методике расследования преступлений. Такое же количество следователей сослались на отсутствие в публикациях четких рекомендаций по соответствующей методике расследования. В.Н. Карагодин отмечает: «… качество научных и учебно-методических работ по методике расследования не устраивает потребителя. Думается, что потребности практики должны определяться, прежде всего, следственными органами на основе обобщения результатов расследования преступлений определенной категории и определения уровня подготовки следственных кадров» [7; с. 64].

Безусловно, качество учебного материала – далеко не основная и не единственная причина проблемы недостаточной квалификации сотрудников. Есть более значимые причины низкой востребованности криминалистической научной продукции. «Согласно статистическим данным, из Следственного комитета России ежегодно увольняется около трети всего состава. То есть каждые 3 года мы видим полностью обновлённый Следственный комитет». С чем связано такое изменение кадрового состава?» – задаются вопросом авторы исследования. «Прежде всего, это ненормированный рабочий день, небольшая заработная плата (для такой ответственной работы), тяжелые условия, постоянное напряжение, много бумажной работы» [8].

Бюрократизация следственной деятельности – отдельная и глобальная проблема, требующая срочных и системных мер. По мнению авторов социологического исследования профессии, в России следователь – в первую очередь «бюрократ», а не «детектив». Способность грамотно оформлять документы следователи сами определяют своим ключевым навыком. 83,2% следователей считают, что способность грамотно провести следственные действия после того, как установлено лицо, подозреваемое в преступлении, и есть главное умение следователя. Только 16,8% ответивших выбрали другой вариант, согласно которому профессионализм следователя состоит в умении устанавливать подозреваемого исходя из результатов следственных действий [9, с. 27]. Если для большинства опрошенных бюрократическая задача – верно оформить документы, важнее интеллектуальной и деятельностной – раскрыть преступление следственными путем, то о каком интересе к научной литературе и вообще – к освоению профессии, может идти речь?! Можно ли по

настоящему способного, а значит весьма творческого человека мотивировать к учебе, заинтересовать в изучении тотально «забюрократизированной», по большей части уныло формализованной профессии?

Вот почему надлежащая мотивация должна лежать в основе методологии, инновационных методов обучения. Эти методы можно условно разделить на общие и частные, где первые включают глобальными концепции и принципы обучения, оптимизацию воспитательно-образовательного процесса, внедрение гуманистических положений, практических и информационных технологий, организация и управления педагогическими процессами. Вторые – частные инновационные методы бывают представлены в форме авторских методик, разработанных на основании современной парадигмы образования и внедренных в воспитательно-образовательный процесс [10].

С точки зрения общих инноваций и в силу прикладного характера науки криминалистики, амбиции ее апологетов и авторов-разработчиков, преподавателей должны простираться в сторону нетривиальной цели – публикации и прочие дидактические средства должны быть самыми практичными среди всех иных наук антикриминального цикла, самыми творческими, увлекательными для молодежи. То есть они должны быть самыми любимыми и популярными со стороны целевой аудитории и, быть может, даже широких слоев населения, как например, детективные фильмы, игры и книги, суть которых – криминалистическое знание. Констатация того, что это пока далеко не так, не требует ни доказательств, ни комментариев…

Далее предложим уже в тезисном виде некоторые общие и частные инновационные методы повышения качества обучения действующих и будущих следователей в условиях глобальной цифровизации:

К числу общих инновационных методов следует отнести:

1) Использование образовательной аудио и видео-продукции, в том числе, на сайтах, в социальных сетях и мессенджерах. В Интернете на текущий момент имеется гигантский объем подкастов и видео-контента: лекции, фильмы, доклады, короткие ролики (самое популярное) и даже онлайн-курсы по криминалистическим и смежным дисциплинам. Однако не все эти продукты цифровизации содержат надлежащую мотивацию к изучению, не все имеют практико-ориентированное содержание и привлекательную форму подачи, доступный и краткий язык, дружественный интерфейс. Автором разработан и размещен в Интернете ряд онлайн-курсов, в частности: «Ошибки и нарушения закона в сфере ОРД» (размещен в системе электронного обучения Санкт-Петербургской академии Следственного комитета России), а также «Защита и обвинение по делам о

коррупционных и должностных преступлениях» [11]. Было бы неэтично хвалится их востребованностью и отзывами. Скажу лишь, что целевая аудитория активно интересуется. Например, уже само название «Защита и обвинение…» (согласованное с маркетологом), как показали опросы, интригует и мотивирует не только адвокатов, но и следователей, стремящихся заглянуть «по ту сторон баррикад», узнать о том, каким будет противодействие расследованию.

2) Использование технологий геймификации в криминалистике, разработка компьютерных игр, специализированных компьютерных программ и мобильных приложений, иных обучающих электронных ресурсов [12; 13; 14]. Ряд таких программ уже разработан. Обычно они направлены на анализ исходной информации о преступлении, выдвижение и проверку типовых версий в ходе расследования [15; 16]. Но дальнейшие успешные разработки могут быть обеспечены только в результате коллективных разработок юристов и IT-специалистов, а также при условии надлежащего, в основном бюджетного финансирования. Ожидание результатов от отдельных энтузиастов – дело бессмысленное и вредное.

3) Междисциплинарность прикладных исследований. Насколько очевидно то, что следователь, прокурор, судья в своей правоприменительной практике не могут разделить мыслительную и практическую деятельность на криминологическую, уголовно-правовую, уголовно-процессуальную и криминалистическую составляющие, настолько же очевидна необходимость разработки и внедрения соответствующих рекомендаций по принципу «разноотраслевое в одном». Впрочем, это, как и остальные тезисы – предмет отдельного, более глубокого исследования.

К числу частных инновационных методов обучения следователей в условиях цифровизации следует отнести:

4) Целенаправленную разработку (на основе вышеизложенных общих методов, современных криминалистических методик расследования так называемых «компьютерных» или кибер-преступлений, а также соответствующих тактических приемов, тактических операций и комбинаций. Например, тактика осмотра и изъятия содержимого мобильных телефонов, иных электронных устройств в современных условиях чрезвычайно актуальное направление прикладных исследований. В целом организационно-технические мероприятия и тактические приемы использования новых программно-технических возможностей при производстве следственных действий – то, чему в обязательном порядке надо обучать следователей.

5) вопросы назначения компьютерных судебных экспертиз, взаимодействия следователя с экспертами и специалистами в области информационных технологий, соответствующими сотрудниками

оперативно-розыскных и оперативно-технических подразделений – насущные проблемы практики. Следователи – это прежде всего юристы, причем со специфическим, преимущественно гуманитарным мышлением. Их невозможно постоянно и эффективно обучать всем аспектам цифровизации. Между тем информационные технологии в настоящее время возникают и устаревают намного быстрее, чем осуществляется обучение. Поэтому надлежащее взаимодействие со спецами – безусловно, обязательная составляющая обучения правоприменителя.

Представлен лишь неполный перечень тезисов, без подробного обоснования. В целом же необходимо готовить следователей к необходимости постоянного обучения, гибкой адаптации к постоянно меняющимся условиям цифровизации. А главное – постоянно мотивировать их к творческой, интересной работе и повышению квалификации. Ученые выделяют несколько этапов цифровизации. Первый – автоматизация за счет внедрения IT-технологий в уголовное судопроизводство, для оптимизации повторяющихся рутинных действий. Второй этап предполагает улучшение и реинжиниринг существующих технологий, применение методов оптимизации процессов и экономии ресурсов (lean-методы). Третий этап цифровизации досудебного производства по уголовным делам связан с появлением новых моделей следственной деятельности и процессов получения доказательств [17; цит. по: 3; с. 38-39]. Уже сами перспективы скорой реализации этих этапов – отличная мотивация для молодежи. Дождемся ли?...

Итак, криминалистика должна постоянно развиваться не только как наука, но и как совокупность интересных, доступно изложенных, прикладных рекомендаций, а также аналогичных дидактических средств. Иначе она малополезна и не будет востребована нашей основной и самой требовательной целевой аудитории - следователями. Предложенные частные и общие инновационные подходы и методы, после обсуждения и оптимизации, детализации в научной сообществе, могут существенным образом повысить качество профессиональной подготовки следователей и иных правоприменителей, обеспечить результативную борьбу с наиболее опасными проявлениями криминальной деятельности. Немаловажно и то, что они могут существенным образом повысить интерес к криминалистике и мотивацию к работе у практикующих коллег и студентов.

Список использованных источников:

1. Нурмагамбетов А.С., Деришев Ю.В. Реформа досудебного производства по новейшему уголовно-процессуальному законодательству Республики Казахстан // Научный вестник Омской академии МВД России. 2015. № 3 (58). С. 26-29.

2. "Паспорт национального проекта "Национальная программа "Цифровая экономика Российской Федерации" (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7).

3. Ищенко П.П. Следственные действия в условиях цифровизации уголовного судопроизводства // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1. С. 30-42.

4. Гармаев Ю.П. Мультимедийные межотраслевые средства предупреждения преступности: перспективы разработки и внедрения // Криминологический журнал Байкальского государственного университета экономики и права. № 3, 2014. С. 71-80.

5. Вележев С.С. Консолидация теории и практики в решении проблем, связанных с юридической ответственностью и наказанием // Администратор суда. 2011. № 1. С. 7-15.

6. Лермонтов М.Ю. Бородино.

7. Карагодин В.Н. Проблемы разработки и внедрения в следственную практику частных методик расследования преступлений / Криминалистические чтения на Байкале – 2015: материалы Междунар. науч.- практ. конф. / Вост.-Сиб. филиал ФГБОУ ВО РГУП; отв. ред. Д.А. Степаненко. – Иркутск, 2015.

8. Катков А.Е., Сухенко Ю.Р. Эмоциональное выгорание у сотрудников Следственного комитета Российской Федерации // COLLOQUIUM-JOURNAL. 2019. № 22-5 (46). С. 45-47.

9. Титаев К.Д. Российский следователь: призвание, профессия, повседневность: монография / К. Титаев, М. Шклярук. – М. : Норма, 2016. 192 с.

10. Инновационные методы обучения. [Электронный ресурс] // Режим доступа: https://spravochnick.ru/pedagogika/teoriya_obucheniya/innovacionnye_metody_obucheniya/ (дата обращения: 03.05.2023).

11. Защита и обвинение по делам о коррупционных и должностных преступлениях / Ю.П. Гармаев. URL: https://clck.ru/32iGmy. – Загл. с экрана. (дата обращения 03.05.2023).

12. Антикоррупционная памятка [Электронный ресурс] // Режим доступа: https://play.google.com/store/apps/details?id=com.wearestars.myapp.production. – Загл. с экрана. (дата обращения 03.05.2023).

13. Мошенничество в автостраховании ОСАГО, ДСАГО, КАСКО [Электронный ресурс] // Режим доступа: https://play.google.com/store/apps/details?id=com.wearestars.avtostrah.production. – Загл. с экрана. (дата обращения 03.05.2023).

14. Присвоение и растрата в сфере страхования [Электронный ресурс] // Режим доступа: https://play.google.com/store/apps/details?id=com.wearestars.strahovanie.production. – Загл. с экрана. (дата обращения 03.05.2023).

15. Пустовая И.Н. Вопросы разработки компьютерных программ расследования преступлений // Правопорядок: история, теория, практика. 2018. №4 (19). С. 26-29.

16. 10 лучших программ для компьютерной криминалистики в 2020 году. [Электронный ресурс] // Режим доступа: https://kriminalisty.ru/top10-digital-forensic-software/. – (дата обращения: 03.05.2023).

17. Государство как платформа: люди и технологии / под ред. М.С. Шклярук. Москва, 2019. 111 с.

УДК 343.48:004

Гулямов Саид Саидахрарович
Заведующий кафедрой «Киберправо» Ташкентского Государственного Юридического Университета, Председатель Совета молодых ученых Академии наук Республики Узбекистан,
доктор юридических наук, профессор,
г. Ташкент, Республика Узбекистан

РОЛЬ ТЕХНОЛОГИЙ В РАСШИРЕНИИ ДОСТУПА К ПРАВОСУДИЮ: ВЗГЛЯД НА БУДУЩЕЕ ПРОЗРАЧНОСТИ СУДЕБНОЙ СИСТЕМЫ

Аннотация. В данной работе исследуется роль технологий и искусственного интеллекта (далее - ИИ) в современной судебной системе и их влияние на доступ к правосудию. Основной акцент делается на возможности ИИ в упрощении и ускорении судебного процесса, улучшении прозрачности и контроля за действиями участников судопроизводства. Автор анализирует преимущества, такие как автоматизация судебного процесса, сокращение сроков и оперативность, а также риски использования ИИ, включая дегуманизацию права и возможность затягивания судебного процесса из-за безграничности анализа данных. В работе рассматриваются методы улучшения конкурентоспособности судейского корпуса и предоставления онлайн-трансляции судебных процессов, а также определение границ применения искусственного интеллекта в судопроизводстве. В целом, работа дает общее представление о перспективе применения технологий и ИИ в судебной системе, возможностях расширения доступа к правосудию и адаптации судебной системы к современным вызовам, сохраняя при этом гуманность и справедливость в процессе принятия решений.

Ключевые слова: искусственный интеллект; ИИ-судья; судопроизводство; онлайн-трансляция; доступность и автоматизация правосудия; право на душевное спокойствие; конкурентоспособность судей; дегуманизация права; безграничность анализа данных; границы применения ИИ.

Аннотация. Жұмыс қазіргі сот жүйесіндегі технологиялар мен жасанды интеллекттің (AI) рөлін және олардың сот төрелігіне қол жеткізуге әсерін зерттейді. Негізгі назар сот процесін жеңілдету және жеделдету, сот ісін жүргізуге қатысушылардың іс-әрекеттерінің ашықтығы мен бақылауын жақсарту үшін АИ мүмкіндігіне аударылады. Автор сот ісін автоматтандыру, мерзімдерді қысқарту және жеделдік сияқты артықшылықтарды, сондай-ақ жасанды интеллектті пайдалану тәуекелдерін, соның ішінде құқықты адамгершіліктен шығаруды және деректерді талдаудың шексіздігіне байланысты сот ісін кейінге қалдыру мүмкіндігін талдайды. Жұмыста судьялар корпусының бәсекеге қабілеттілігін жақсарту және сот процестерін онлайн трансляциялауды ұсыну әдістері, сондай-ақ сот ісін жүргізуде жасанды интеллектті қолдану шекараларын анықтау қарастырылады. Тұтастай алғанда, жұмыс сот жүйесінде технологиялар мен жасанды интеллектті қолдану перспективасы, сот төрелігіне қол жетімділікті кеңейту мүмкіндіктері және шешім қабылдау процесінде адамгершілік пен әділеттілікті сақтай отырып, сот жүйесін заманауи сынақтарға бейімдеу туралы жалпы түсінік береді.

Түйінді сөздер: жасанды интеллект; ЖИ-төреші; сот ісін жүргізу; онлайн-көрсетілім; қол жетімділік және сот төрелігін автоматтандыру; жан тыныштығына

құқық; төрешілердің бәсекеге қабілеттілігі; құқықты адамсыздандыру;деректерді талдаудың шексіздігі; ЖИ қолдану шекаралары.

Annotation. This paper examines the role of technologies and artificial intelligence (AI) in the modern judicial system and their impact on access to justice. The main focus is on the AI's ability to simplify and speed up the judicial process, improve transparency and control over the actions of participants in the proceedings. The author analyzes the advantages, such as automation of the judicial process, reduction of time and efficiency, as well as the risks of using AI, including dehumanization of law and the possibility of delaying the trial due to the limitlessness of data analysis. The paper discusses methods for improving the competitiveness of the judiciary and providing online broadcasting of trials, as well as defining the boundaries of the use of artificial intelligence in court proceedings. In general, the work gives a general idea of the prospects for the use of technologies and AI in the judicial system, the possibilities of expanding access to justice and adapting the judicial system to modern challenges, while maintaining humanity and fairness in the decision-making process.

Keywords: artificial intelligence; AI- judge; legal proceedings; online-broadcast; availability and automation of justice; the right to peace of mind; competitiveness of judges; dehumanization of law; the limitlessness of data analysis; boundaries of AI application.

Введение. Современный мир испытывает значительное влияние информационных технологий и искусственного интеллекта (далее – ИИ) на различные сферы общественной жизни. Судебная система не является исключением и уже сейчас мы наблюдаем, как цифровые инновации начинают проникать в механизмы предоставления правосудия. В связи с этим возникает необходимость исследования и анализа возможностей и вызовов, связанных с применением технологий и ИИ в расширении доступа к правосудию [1].

В настоящее время существует ряд проблем, с которыми сталкивается традиционная судебная система, такие как ограниченный доступ к правосудию, затягивание судебного процесса, неоднородность качества судебных решений и возможное воздействие человеческого фактора на исход дела. В этом контексте возникает актуальный вопрос: могут ли информационные технологии и искусственный интеллект способствовать улучшению ситуации и предложить альтернативные решения для современных проблем в сфере правосудия?

Исследования в области применения технологий и ИИ в судебной системе набирают обороты, многие ученые и эксперты утверждают, что внедрение новых технологий может иметь положительное влияние на качество и доступность судебного процесса. Вместе с тем, эти инновации предъявляют определенные вызовы, такие как дегуманизация права, проблемы кибербезопасности, а также необходимость адаптации законодательства и инфраструктуры судебной системы к новым технологическим реалиям.

Целью данной статьи является анализ возможностей и вызовов, связанных с использованием технологий и искусственного интеллекта в судопроизводстве, а также обсуждение возможных путей развития

прозрачной судебной системы, основанной на принципах цифрового правосудия. Автор статьи обращает внимание на актуальные проблемы, связанные с использованием ИИ и технологий в судебной системе, а также рассматривает потенциальные преимущества и недостатки различных подходов к их внедрению.

В статье освещаются темы, такие как автоматизация судебного процесса, применение алгоритмов ИИ для анализа и решения правовых вопросов, использование информационных технологий для ускорения и упрощения доступа к правовой информации и услугам, а также вопросы прозрачности и демократизации судебной системы благодаря внедрению технологий.

В дополнение к этому, в статье обращено внимание на некоторые из возможных рисков и проблем, которые могут возникнуть при применении ИИ и технологий в судебной системе, такие как вопросы конфиденциальности и защиты данных, кибербезопасности, этических аспектов использования ИИ и потенциального влияния на принципы гуманности и справедливости в судопроизводстве. Автор также предлагает рекомендации и стратегии для преодоления этих проблем, предложения по разработке более эффективной и прозрачной судебной системы с использованием технологий и искусственного интеллекта.

Для достижения цели исследования в данной работе проводится анализ существующей литературы, зарубежного опыта и примеров применения технологий в судебной системе, а также проводится исследование и разработка прогнозов относительно будущего развития прозрачности судебной системы с использованием ИИ и технологий. В результате работы предлагается общая концепция «Теории прозрачности судопроизводства», которая сможет послужить основой для дальнейших исследований и разработки новых подходов к внедрению информационных технологий и искусственного интеллекта в судебную систему.

Методология исследования

В рамках данного исследования была использована симбиотическая методология, включающая изучение литературы, анализ нормативных актов, применение методов синтеза и анализа для систематизации и обобщения полученной информации.

Для начала, в целях оценки текущего состояния знаний о применении технологий и искусственного интеллекта в судебной системе, был проведен обширный обзор существующей научной литературы [2-7], включая статьи [8-11], монографии [12-15] и исследовательские отчеты [16-18]. Это позволило выявить основные тенденции, достижения, а также потенциальные проблемы и риски, связанные с использованием технологий в судопроизводстве.

Затем проводился анализ нормативных актов, регулирующих применение технологий в судебной системе, как на национальном, так и

на международном уровнях [19-22]. Это позволило изучить существующие правовые рамки и определить возможные коллизии в законодательстве, которые могут влиять на эффективность и прозрачность судебной системы при использовании информационных технологий.

Для сбора и систематизации информации были выбраны и использованы методы синтеза и анализа. Синтез позволил объединить различные идеи и подходы, предложенные в исследованиях и нормативных актах, сформулировать комплексное представление о применении технологий и искусственного интеллекта в судебной системе. Метод анализа использовался для выделения ключевых аспектов, рисков и проблем, а также для определения возможных стратегий и рекомендаций по преодолению возникающих трудностей.

Таким образом, на основе проведенного исследования, удалось разработать общую концепцию «Теории прозрачности судопроизводства», которая сможет послужить отправной точкой для дальнейших исследований и разработки новых подходов к внедрению информационных технологий и искусственного интеллекта в судебную систему.

Результаты исследования

Результаты исследования, представленные в данной статье, нацелены на освещение ряда ключевых аспектов, таких как: теория прозрачности судопроизводства, сопровождение дела до его логического завершения (включая принятие заявления, медиацию, судебный процесс, разрешение проблемы на Верховной коллегии суда и исполнение судебного решения), возникновение новых прав человека и положительные аспекты **«**Теории прозрачности судопроизводства» (предсказуемое право, моделируемое право), право на душевное спокойствие, онлайн-трансляция судебного процесса, конкурентоспособность судейского корпуса, доступность правосудия, автоматизация системы правосудия и сокращение сроков, процесс выявления проблемы и направление проблемы органам государственной власти, а также мониторинг всего процесса и логическое завершение дела.

Кроме того, результаты исследования включают анализ потенциальных рисков, связанных с развитием судопроизводства и внедрением ИТ-технологий, в частности дегуманизацию права, безграничность анализа данных, технические риски и неготовность традиционной судебной системы к вызовам информационных технологий.

Теория прозрачности судопроизводства

Основным движущим фактором Теории виртуального парламента является автоматизация системы правосудия и внедрение искусственного интеллекта, что способствует практической реализации

принципа прозрачности, обеспечению свободного доступа к правосудию, сокращению времени и издержек судебного процесса, а также сопровождению дела до его логического завершения.

Алгоритм действий для запуска и эффективной работы судебной системы включает разработку программных решений: онлайн подачи заявления и разработку «судьи-симулятора» [23], основными задачами которых являются проверка полноты и достоверности иска, проведение медиации, передача дела на рассмотрение в суд и, что наиболее важно, сопровождение иска до его логического завершения.

Сопровождение дела до его логического завершения

Искусственный интеллект обеспечивает сопровождение дела до его логического завершения, выполняя контроль над: приемом заявления, медиацией, судебным процессом, разрешением проблемы на уровне Верховной коллегии суда, разрешением проблемы на законодательном уровне и исполнением судебного решения.

1. Принятие заявления

Важным этапом является объединение официальных сайтов всех судов и правоохранительных органов государства в единую интерактивную платформу, что упростит процесс поиска и подачи онлайн-заявления. На данном этапе функция искусственного интеллекта заключается в принятии заявления от заявителя в соответствии с требованиями законодательства. ИИ помогает заявителю сформулировать заявление, задавая ряд указательных вопросов и запросив соответствующие документы для рассмотрения.

Все предоставляемые документы должны иметь цифровой характер, за исключением случаев, где цифровизация пока недоступна, например, вещественные доказательства или физическое насилие.

После заполнения необходимых полей заявления, ИИ принимает его к рассмотрению и отправляет запрос на «предсказуемое» решение к «судье-симулятору». На основании полученных результатов заявитель имеет право отказаться от дальнейшего рассмотрения заявления или продолжить процесс [24].

На этом этапе искусственный интеллект анализирует причины отказа истцу, проверяет криминальный характер представленных доказательств, выявляет причину, не позволившую закончить заполнение заявления, принимает меры в случае выявления насильственных действий против истца, направляет незавершенное заявление в разделы «криминальное» или «семейное» правоохранительным органам для проверки и принятия профилактических мер против насилия и явных нарушений прав человека. Кроме того, ИИ выявляет статистические проблемы, как правовые, так и технические, которые мешают принимать заявления, направляет выявленные проблемы в соответствующие органы для их разрешения и информирует стороны об устранении проблемы.

Таким образом, искусственный интеллект на этапе принятия заявления выполняет множество функций, которые направлены на упрощение процесса подачи заявления, обеспечение его полноты и достоверности, а также на выявление и решение возникающих проблем, связанных с судопроизводством и защитой прав человека [25].

2. Медиация

Полученное заявление, сопровождаемое результатами прогнозируемого решения, отправляется ответчику для рассмотрения. Ответчику предоставляется срок для представления своих доводов в противовес заявленных истцом требований. Искусственный интеллект вносит представленные доводы в базу данных судьи-симулятора и отправляет результаты прогнозируемого нового решения истцу для дальнейшего анализа.

Данная процедура фактически является медиацией и проводится до тех пор, пока решение судьи-симулятора не удовлетворит обе стороны. В ходе медиации искусственный интеллект анализирует причины неудовлетворенности сторон, проверяет криминальный характер представленных доказательств, выявляет пробелы и противоречия в законодательстве, определяет статистические проблемы сторон в медиационном процессе и направляет обнаруженные проблемы в соответствующие органы для разрешения. ИИ также информирует стороны о решении проблемы, контролирует исполнение утвержденного решения обеими сторонами и т. д.

3. Судебный процесс

Если одна из сторон считает, что решение судьи-симулятора содержит правовые или технические недостатки или технологические проблемы, она может потребовать рассмотрение дела реальным судьей. После тщательного изучения дела судья выносит собственное решение, объясняя при этом неправильность решения судьи-симулятора [26].

Если в судебном процессе обнаруживаются правовые недочеты, проблемы, коллизии или противоречия в законодательстве, и судья не может принять справедливое и обоснованное решение, то дело приостанавливается. Проблема передается искусственному интеллекту в Верховную коллегию суда для разрешения, соблюдая все нормы защиты данных.

Если при рассмотрении дела судьей не выявляется веских оснований для изменения решения судьи-симулятора, то суд утверждает решение судьи-симулятора и привлекает к ответственности сторону за необоснованность предъявленных доводов.

В рамках судебного процесса искусственный интеллект контролирует и информирует стороны о сроках всех судебных процедур, проверяет криминальный характер представленных сторонами новых доказательств, ведет протоколы заседаний суда и выполняет роль

судьи-симулятора. Искусственный интеллект также может служить научным и практическим советником судье, направлять выявленные проблемы и противоречия в законодательстве в Верховную коллегию суда для разрешения, проводить мониторинг решения вопроса в формате онлайн, информировать стороны об устранении проблемы и контролировать исполнение судебного решения и т. д.

4. Разрешение проблемы на Верховной коллегии суда

В данном случае искусственный интеллект осуществляет онлайн мониторинг рассмотрения дела Верховной коллегией суда, может предложить обоснованные варианты применения иностранного права по аналогии, анализирует и обобщает мнение всего состава судей, ведет протоколы заседаний суда и выполняет роль судьи-симулятора. При положительном решении проблемы, искусственный интеллект логически заканчивает судебный процесс, вносит нормативный акт в свою базу данных, а при отрицательном результате передает вопрос на дальнейшее обсуждение на законодательном уровне.

5. Разрешение проблемы на законодательном уровне

Здесь искусственный интеллект ведет мониторинг сроков рассмотрения вопроса в виртуальном парламенте, информирует стороны об устранении проблемы и контролирует исполнение судебного решения [27].

6. Исполнение судебного решения

В данном контексте искусственный интеллект, при возможности решения вопроса на цифровом уровне, исполняет решение суда в качестве судоисполнителя (онлайн-списание долгов, проведение онлайн-аукционов цифровой недвижимости и т. д.). ИИ также осуществляет онлайн мониторинг сроков и деятельности судебных исполнителей, выявляет проблемы, создающие препятствия для исполнения правосудия, направляет обнаруженные проблемы в соответствующие органы для разрешения и информирует стороны об устранении проблемы.

Возникновение новых прав человека и положительные аспекты

Теории прозрачности судопроизводства

Предсказуемое право

Предсказуемое право означает, что право на предсказуемое правосудие должно быть основано исключительно на нормах закона, без учета личных предпочтений и произвольных решений. Это подразумевает, что при предоставлении верных данных заявителем существуют основания для защиты его прав в соответствии с законодательством. В случае принятия противоположного решения искусственным интеллектом, судья обязан обосновать его [28].

Моделируемое право

Моделируемое право представляет собой право на получение бесплатного правового консультанта для моделирования

(прогнозирования) предстоящего судебного процесса. На основе введенных новых данных, искусственный интеллект может предварительно моделировать различные результаты предсказуемых решений и предоставлять правовые советы по правильному оформлению доказательной базы. Благодаря этой бесплатной функции, любой человек, даже не имеющий юридического образования, может воспользоваться услугами ИИ. Это поможет снизить расходы на дорогое адвокатское сопровождение [29].

Право на душевное спокойствие

Искусственный интеллект не будет принимать к рассмотрению заявления без достаточных оснований и доказательств вины ответчика. Доводы и факты, представленные истцом, проверяются в процессе принятия заявления, а не в ходе традиционного судебного процесса [30]. Это означает, что у ответчика появляется право на защиту от необоснованных исков, вызванных актами неприязни или другими основаниями. Таким образом, реализуется принцип презумпции невиновности, когда бремя доказательства лежит на истце, а также право на душевное спокойствие.

Онлайн-трансляция судебного процесса

При соблюдении всех процедур защиты данных, онлайн трансляция позволит СМИ и всем заинтересованным лицам следить за судебным процессом. Это способствует достижению прозрачности, антикоррупционной политики, обоснованности и адекватности судебных решений, а также ограничению внешнего воздействия на исход правосудия [31].

Конкурентоспособность судейского корпуса

Судьи будут вынуждены конкурировать с искусственным интеллектом в принятии альтернативных решений. Это означает, что судье необходимо обосновать свое научно-практическое решение, отличное от решения, предложенного искусственным интеллектом. Государство и общество получат право оценивать действия и принятые решения судьи с правовой и социальной точки зрения. В результате судьи должны будут постоянно работать над повышением своей квалификации.

Доступность правосудия

Применение онлайн заявления обеспечит свободный доступ к справедливому правосудию, устранит границы правовой грамотности, пространственных и временных ограничений, а также различных социальных и материальных неравенств [32].

Автоматизация системы правосудия и сокращение сроков

Искусственный интеллект позволит быстро разрешать множество стандартных социально-бытовых споров в сфере гражданского права (раздел имущества, наследство и др.), коммерческого права (договорные отношения, защита прав потребителей и др.), очевидно

нарушенные права человека, административные тяжбы (штрафы, налоги, оплата коммунальных услуг и др.) и другие статистические споры, не требующие человеческого фактора и решаемые на нормативном уровне [33]. Автоматизация системы правосудия приведет к сокращению сроков рассмотрения дел и повышению эффективности судебной системы.

Процесс выявления проблемы и направление проблемы органам государственной власти

Искусственный интеллект будет способен определить практические проблемы материального и процессуального права, выявить противоречия в законодательстве и нарушения прав человека, а также собирать и обобщать статистические данные. Кроме того, ИИ сможет оперативно направлять выявленные проблемы на решение в соответствующие органы и контролировать их разрешение на законодательном уровне.

Мониторинг всего процесса и логическое завершение дела

Искусственный интеллект также позволит отслеживать законность всех действий участников судебного процесса, заблаговременно предупреждать о нарушениях сроков судопроизводства и нормотворчества, обеспечивать прозрачность и справедливость судебного процесса, и в итоге завершать судебное дело, включая его исполнение.

Риски в теории прозрачности судопроизводства

1. Дегуманизация права

Некоторые ученые высказывают опасения о дегуманизации судебной системы в случае полной автоматизации судебных решений, поскольку в этом случае будет отсутствовать принцип гуманности, который является неотъемлемой частью любого принятого судебного решения [25]. В связи с ограничениями искусственного интеллекта в области анализа эмоций, переживаний, духовного состояния и других качеств, присущих только человеку, необходимо определить границы применения ИИ в судопроизводстве, в частности, сохранить право принятия решения настоящим судьей в сфере семейных отношений, уголовного преследования и религии.

Однако, следует учесть, что все нормативные акты, заложенные в базу данных ИИ, были приняты людьми, исходя из позиций гуманности. ИИ, посредством судьи-симулятора, применяет материальные и процессуальные нормы аналогично настоящему судье. При этом большинство судебных дел не требует анализа состояния человека, и применяются ранее принятые судебные решения и нормы законодательства автоматически, что позволит сократить человеческий фактор в принятии судебных решений.

2. Безграничность анализа данных

В процессе поиска решения задачи, искусственный интеллект имеет возможность безграничного анализа больших данных в киберпространстве, что может затянуть судебный процесс. В этой связи, следует определить и ограничить рамки поиска решения ИИ на всех стадиях судопроизводства и нормотворчества, как во времени, так и пространстве.

3. Технические риски

Технические риски искусственного интеллекта возникают из-за его непосредственной связи с информационными технологиями, линиями связи, программным обеспечением, электричеством и другими техническими средствами. Возможны риски, связанные со взломом программного продукта, кражей данных, вирусами, несанкционированными изменениями в базе данных, а также проблемами, связанными с человеческим фактором [28].

При использовании искусственного интеллекта кибербезопасность становится особенно важной. Современные технологии позволяют внедрять в алгоритмы ИИ постоянное отслеживание незаконного вторжения в систему, применять различные технические средства и обеспечивать необходимую степень безопасности [26].

4. Неготовность традиционной судебной системы к ИТ-вызовам

Традиционная судебная система может оказаться не готовой к вызовам информационных технологий. Цифровизация и виртуализация расширяют диапазон технических процедур в судебном процессе, что требует новых правовых рамок и технологических решений. Примеры таких вызовов включают возникновение новых прав сторон, требующих регулирования; отсутствие четких правомочий ИИ; необходимость крупных капиталовложений для технологического решения, включая сканирование ранее рассмотренных судебных дел; неготовность части взрослого населения к радикальным ИТ-изменениям; неудовлетворительное состояние действующего законодательства; потребность в технологическом обновлении всех государственных органов, функции, которых напрямую или косвенно связаны с новым судопроизводством; и невозможность оцифровки некоторых доказательств.

Однако считается, что эти риски могут быть разрешены, поскольку они зависят от материальных затрат и мотивации общества [33]. Финальным этапом теории прозрачности судопроизводства должно становиться принятие Кодекса цифрового правосудия, целью которого является обеспечение правовых рамок для новой прозрачной судебной системы, основанной на информационных технологиях и защите прав человека. Данный Кодекс предусматривает регулирование применения цифровых технологий в судопроизводстве и будет учитывать возникающие вызовы, связанные с информационными технологиями и кибербезопасностью.

В процессе внедрения цифрового правосудия следует учесть опыт и ошибки прошлого, а также стремиться к постоянному совершенствованию системы, учитывая интересы всех участников судебного процесса и общества в целом. Важно также сбалансировать применение искусственного интеллекта с сохранением человеческого элемента и гуманности в судебной системе, чтобы обеспечить справедливость и защиту прав и свобод каждого человека [26].

В результате реализации теории прозрачности судопроизводства возможно создание судебной системы, которая будет более доступной, эффективной и справедливой для всех участников, обеспечивая при этом высокий уровень защиты информации и кибербезопасности.

Обсуждение результатов

Анализ результатов показывает, что применение технологий и искусственного интеллекта в судопроизводстве имеет ряд преимуществ, таких как повышение эффективности, ускорение процесса, снижение человеческого фактора и более широкий доступ к правосудию. Однако, важно учитывать и потенциальные риски, такие как дегуманизация права, технические проблемы, кибербезопасность и юридические аспекты использования искусственного интеллекта в судебной системе.

Внедрение технологий в судебную систему требует глубокого осознания их возможностей и ограничений, а также разработки подходящих правовых рамок и норм, способных обеспечить справедливый и сбалансированный подход к использованию искусственного интеллекта в судопроизводстве.

Заключение. Искусственный интеллект и технологии могут стать значительным инструментом для повышения прозрачности, доступности и справедливости судебной системы в будущем. Вместе с тем, критически важно осознавать и контролировать возможные риски и проблемы, связанные с их использованием в судопроизводстве. Обеспечение кибербезопасности, разработка правовых рамок, адаптация традиционной судебной системы к вызовам информационных технологий и учет мнений и опыта всех заинтересованных сторон – ключевые аспекты, которые следует учитывать при внедрении новых технологий в судебную систему.

Принятие Кодекса цифрового правосудия, цель которого заключается в обеспечении правовых рамок для новой прозрачной судебной системы, основанной на информационных технологиях и защите прав человека, является важным шагом в этом направлении. Интеграция искусственного интеллекта и технологий в судопроизводство может привести к значительному прогрессу в доступе к правосудию и улучшению качества судебных решений, если их внедрение будет проходить с учетом всех потенциальных вызовов и возможностей.

Список использованных источников:

1. Katz, D. M. (2017). Artificial Intelligence and Legal Technology: A New Paradigm for Access to Justice. In: Livermore, M.A., & Rockmore, D.N. (Eds.), Law as Data: Computation, Text, and the Future of Legal Analysis. Santa Fe Institute Press. [Electronic resource] – Access mode: https://www.elevenjournals.com/ (Access date: 02.05.2023.).
2. Remus, D., & Levy, F. S. (2014). Can Robots Be Lawyers? Computers, Lawyers, and the Practice of Law. Georgetown Journal of Legal Ethics, 30, 501-558. [Electronic resource] – Access mode: https://doi.org/10.2139/ssrn.2701092 (Access date: 02.05.2023.).
3. Surden, H. (2014). Machine Learning and Law. Washington Law Review, 89(1), 87-115. [Electronic resource] – Access mode: https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4799&context=wlr (Access date: 02.05.2023.).
4. Gulyamov, S., Rustambekov, I., Narziev, O., & Xudayberganov, A. (2021). Draft Concept of the Republic of Uzbekistan in the Field of Development Artificial Intelligence for 2021-2030. Yurisprudensiya, 1, 107-21. [Electronic resource] – Access mode: https://www.researchgate.net/publication/351658151_DRAFT_CONCEPT_OF_THE_REPUBLIC_OF_UZBEKISTAN_IN_THE_FIELD_OF_DEVELOPMENT_ARTIFICIAL_INTELLIGENCE_FOR_2021-2030 (Access date: 02.05.2023.).
5. Saidakhrarovich, G. S., & Sokhibjonovich, B. S. (2022). Strategies and future prospects of development of artificial intelligence: world experience. World Bulletin of Management and Law, 9, 66-74. [Electronic resource] – Access mode: https://scholarexpress.net/index.php/wbml/article/view/841 (Access date: 02.05.2023.).
6. Katz, D. M. (2013). Quantitative Legal Prediction – Or – How I Learned to Stop Worrying and Start Preparing for the Data Driven Future of the Legal Services Industry. Emory Law Journal, 62(4), 909-966. [Electronic resource] – Access mode: https://ssrn.com/abstract=2187752 (Access date: 02.05.2023.).
7. Gulyamov, S., & Yusupov, S. (2022). Issues of Legal Regulation of Robotics in the Form of Artificial Intelligence. European Multidisciplinary Journal of Modern Science, 5, 440-445. [Electronic resource] – Access mode: https://emjms.academicjournal.io/index.php/emjms/article/view/297 (Access date: 02.05.2023.).
8. Гулямов, С. (2022). Digitalization of international arbitration and dispute resolution by artificial intelligence. Гулямов Саид Саидахрарович, (1). [Electronic resource] – Access mode: https://scholarexpress.net/index.php/wbml/article/view/848 (Access date: 02.05.2023.).
9. Alarie, B., Niblett, A., & Yoon, A. (2018). How Artificial Intelligence Will Affect the Practice of Law. University of Toronto Law Journal, 68(1), 106-124. [Electronic resource] – Access mode: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066816 (Access date: 02.05.2023.).
10. Saidakhrarovich, G.S., & Tursunovich, K. O. (2022). DIGITAL FUTURE & CYBER SECURITY NECESSITY. World Bulletin of Management and Law, 10, 31-45. [Electronic resource] – Access mode: https://scholarexpress.net/index.php/wbml/article/view/948 (Access date: 02.05.2023.).
11. Arntz, M., Gregory, T., & Zierahn, U. (2016). The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis. OECD Social, Employment, and Migration Working Papers, No. 189. [Electronic resource] – Access mode: https://doi.org/10.1787/5jlz9h56dvq7-en (Access date: 02.05.2023.).
12. Dabney, D.P. The Expanding Role of Artificial Intelligence in Legal Research. The Law Librarian, №42 (2), 2011. С.67-72.
13. Browning, J. (2018). Legal Tech, Smart Contracts and Blockchain. Singapore Academy of Law Journal, 30, 26-43. [Electronic resource] – Access mode:

https://www.amazon.com/Contracts-Blockchain-Perspectives-Business-Innovation/dp/9811360855 (Access date: 02.05.2023.).
14. Susskind, R.E., & Susskind, D. (2015). The Future of the Professions: How Technology Will Transform the Work of Human Experts. Oxford University Press. [Electronic resource] – Access mode: https://academic.oup.com/book/40589 (Access date: 02.05.2023.).
15. Fenwick, M., Vermeulen, E.P., & Kaal, W.A. (2017). Regulation Tomorrow: What Happens When Technology Is Faster than the Law? American University Business Law Review, 6 (3), 561-594. [Electronic resource] – Access mode: https://ssrn.com/abstract=3018212 (Access date: 02.05.2023.).
16. Baker, C. E. (2018). Юридическая индустрия для контрактной аналитики с поддержкой ИИ: анализ рынка. ABA Journal of Labor & Employment Law, 33(3), 321-336. [Электронный ресурс] – Режим доступа: https://ssrn.com/abstract=3118341 (Access date: 02.05.2023.).
17. Marra, W.P., & McInnis, T.J. The Impact of AI on the Practice of Law. The Judges' Journal, №54 (3), 2015. С.8-12.
18. Brink, D. V. (2018). Artificial Intelligence and the Legal Profession: A Blessing or a Curse? Legal Tech Weekly. [Electronic resource] – Access mode: https://nqsolicitors.com/blog/is-ai-a-blessing-or-a-curse-for-junior-lawyers/ 02.05.2023.).
19. European Commission for the Efficiency of Justice (CEPEJ). (2018). European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment. [Electronic resource] – Access mode: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (Access date: 02.05.2023.).
20. United Nations. (2018). Guidelines for the Regulation of Computerized Personal Data Files. A/RES/45/95. [Electronic resource] – Access mode: https://undocs.org/A/RES/45/95 (Access date: 02.05.2023.).
21. U.S. Congress. (2017). H.R.4174 - Foundations for Evidence-Based Policymaking Act of 2018. 115th Congress (2017-2018). [Electronic resource] – Access mode: https://www.congress.gov/bill/115th-congress/house-bill/4174 (Access date: 02.05.2023.).
22. Australian Government. (2017). Artificial Intelligence: Australia's Ethics Framework. Department of Industry, Innovation, and Science. [Electronic resource] – Access mode: https://consult.industry.gov.au/ (Access date: 02.05.2023.).
23. Zeiler, K., & Eder, S.G. (2019). Онлайн-разрешение споров и искусственный интеллект. Международный журнал онлайн-разрешения споров, 6(1), 5-26. [Электронный ресурс] – Режим доступа: https://www.tandfonline.com/doi/full/10.1080/13600834.2022.2088060 (дата обращения: 02.05.2023 г.).
24. Katz, D.M. (2017). Legal Informatics. Cambridge University Press. [Electronic resource] – Access mode: https://www.cambridge.org/core/books/legal-informatics/37956B00CC40F2803B77A164CD970757 (Access date: 02.05.2023.).
25. Remus, D., & Levy, F.S. (2016). Могут ли роботы быть юристами? Компьютеры, юристы и юридическая практика. Джорджтаунское юридическое технологическое обозрение, 30(2), 321-336. [Электронный ресурс] – Режим доступа: https://go.gale.com/ps/i.do?id=GALE%7CA514460996&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=10415548&p=AONE&sw=w&userGroupName=anon%7E73bea7b4 (дата обращения: 02.05.2023 г.).
26. Surden, H. (2014). Machine Learning and Law. Washington Law Review, 89(1), 87-115. [Electronic resource] – Access mode: https://digitalcommons.law.uw.edu/wlr/vol89/iss1/5/ (Access date: 02.05.2023.).
27. Hagan, M. (2018). Финал основанного на интуиции анализа политики высокого уровня: искусственный интеллект и верховенство закона. Georgetown Law

Technology Review, 2(1), 1-32. [Электронный ресурс] – Режим доступа: https://georgetownlawtechreview.org/ (Access date: 02.05.2023.).

28. Chen, D., & Halim, R. Искусственный интеллект и принятие судебных решений: исследовательская программа. Документ Чикагского университета по публичному праву и теории права №692, 2018.

29. Smith, A. (2019). ИИ и юридическая практика: комплексный взгляд на принятие и реализацию. Новости юридических технологий. [Электронный ресурс] – Режим доступа: https://www.researchgate.net/publication/338163462_Artificial_intelligence_in_the_legal_sector_pressures_and_challenges_of_transformation (дата обращения: 02.05.2023 г.).

30. Ruan, N. Искусственный интеллект в мире гражданского судопроизводства. Ежеквартальное издание «Гражданское правосудие», №38 (2), 2019. С.131-154.

31. Graef, I., Husovec, M., & Purtova, N. (2018). Переносимость данных и управление данными: уроки для новой концепции в законодательстве ЕС. Исследовательская работа Тилбургской юридической школы No 22. [Электронный ресурс] – Режим доступа: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071875 (дата обращения: 02.05.2023 г.).

32. Staudt, R.C., & Medeiros, A.P. (2015). Access to Justice and Technology Clinics: A 4% Solution. Chicago-Kent Law Review, 88(3), 695-732. [Electronic resource] – Access mode: https://scholarship.kentlaw.iit.edu/cklawreview/vol88/iss3/3 (Access date: 02.05.2023.).

33. Susskind, R. (2019). Online Courts and the Future of Justice. Oxford University Press. [Electronic resource] – Access mode: https://global.oup.com/academic/product/online-courts-and-the-future-of-justice-9780192849304?cc=uz&lang=en& (Access date: 02.05.2023.).

34. Brownsword, R. (2016). In the Year 2061: From Law to Technological Management. Law, Innovation and Technology, 8(1), 1-51. [Electronic resource] – Access mode: https://www.tandfonline.com/doi/abs/10.1080/17579961.2015.1052642?journalCode=rlit20 (Access date: 02.05.2023.).

УДК 343.985:336.741.24

Калиев Аскар Абужанович
Доцент кафедры специальной подготовки по противодействию глобальным угрозам Института повышения профессионального уровня Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан
г. Астана, Республика Казахстан

ПРОБЛЕМНЫЕ ВОПРОСЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

Аннотация. В статье описываются различные способы использования криптовалют в преступных целях. Рассмотрены проблемы и вызовы, с которыми сталкиваются правоохранительные органы, борясь с использованием криптовалют в криминальной сфере. Автор статьи предлагает некоторые способы борьбы с использованием криптовалют в преступной деятельности, такие как регулирование, мониторинг криптовалютных бирж и использование технологических инструментов. В целом, статья представляет актуальное исследование, которое поможет понять роль криптовалют в преступной деятельности и как этому противостоять.

Ключевые слова: криптовалюты; транзакции; расследование; правовое регулирование; блокчейн, информационно-коммуникационные технологии; интернет; цифровые активы.

Аннотация. Мақалада криптовалюталарды қылмыстық мақсатта пайдаланудың әртүрлі тәсілдері сипатталған. Қылмыстық салада криптовалюталарды қолданумен күресу кезінде құқық қорғау органдарының алдында тұрған мәселелер мен қиындықтар қарастырылады. Мақала авторы криптовалюталарды қылмыстық әрекеттерде пайдаланумен күресудің кейбір жолдарын ұсынады, мысалы, реттеу, криптовалюталық биржаларды бақылау және технологиялық құралдарды пайдалану. Жалпы, мақалада криптовалюталардың қылмыстық әрекеттегі рөлін және оған қарсы тұру жолдарын түсінуге көмектесетін заманауи зерттеулер ұсынылған.

Түйінді сөздер: криптовалюталар; транзакциялар; тергеу; құқықтық реттеу; блокчейн, ақпараттық және коммуникациялық технологиялар; интернет; цифрлық активтер.

Annotation. The article describes various ways of using cryptocurrencies for criminal purposes. The problems and challenges faced by law enforcement agencies fighting the use of cryptocurrencies in the criminal sphere are considered. The author of the article suggests some ways to combat the use of cryptocurrencies in criminal activities, such as regulation, monitoring of cryptocurrency exchanges and the use of technological tools. In general, the article presents an up-to-date study that will help to understand the role of cryptocurrencies in criminal activity and how to resist it.

Keywords. cryptocurrencies, transactions, investigation, legal regulation, blockchain, information and communication technologies, Internet, digital assets.

Введение. Современные технологии и интернет способствовали миграции большей части правонарушителей в виртуальный мир, где

основным способом оплаты и заработка стала криптовалюта, такие как биткоин, эфириум и другие. При этом правоохранительные органы отмечают трудности при расследовании таких преступлений, особенно при рассмотрении вопроса об обнаружении, наложении ареста и конфискации криптовалюты.

Основная часть. Что собой представляет криптовалюта? В разных источниках дается множество различных определений данному термину. Криптовалюта – вид цифрового знака (токена), представляющий собой запись в реестре блоков транзакций (блокчейне), иной распределённой базе данных и принимаемый в качестве средства обмена и (или) единицы учета и (или) средства хранения (накопления) стоимости [1, с.7]. Криптовалюта – это вид цифровой валюты, защищенной от подделки, которую можно хранить в электронных кошельках, а также переводить из одного кошелька в другой [2, с.433]. Иными словами, криптовалюты - это цифровые инструменты, созданные с целью облегчить электронный обмен между людьми. Однако из-за своих уникальных свойств их стали применять в преступной деятельности.

Преступники с помощью криптовалюты скрывают свои денежные потоки, которые потом перемещают в криптокошельки, зарегистрированные в иностранных юрисдикциях, оплачивают запрещенные товары и услуги, используют их при совершении различных видов и форм мошенничеств, таких как вымогательство, фишинг. В последнее время они стали популярны при передаче и получении взятки, так как эти операции анонимны и «безопасны» для правонарушителей [3, с.20].

Криптовалюты обладают рядом преимуществ по сравнению с традиционными финансовыми инструментами, что делает их более привлекательными для преступных групп. К таким преимуществам можно отнести:

1. Анонимность – транзакции с использованием криптовалют не требуют никакой личной идентификации, что делает их идеально подходящими для использования преступниками;

2. Необратимость – криптовалютные транзакции не могут быть отозваны или обратимы, что защищает мошенников от возврата похищенных ими денег;

3. Быстрота – транзакции с использованием криптовалют происходят быстро и без участия банков, что ускоряет все процессы и защищает от отслеживания.

Расследование такого рода преступлений, связанных с использованием криптовалют, требует особых знаний и опыта.

В первую очередь, следователю необходимо хорошо понимать принципы и функционирование криптовалютных технологий, уметь анализировать транзакции в блокчейне, отслеживать потоки

криптовалютных средств, а также оперировать понятиями, связанными с криптовалютными биржами, кошельками, майнингом и прочими [4, с.15].

Кроме того, следователь должен быть знаком с международным законодательством, связанным с криптовалютами, так как в ряде случаев расследование может пересекаться с работой правоохранительных органов из других стран, законодательство которых отличается от казахстанского.

Одним из ключевых методов расследования криптовалютных преступлений является проведение анализа данных. Следователю необходимо уметь собирать, анализировать и коррелировать множество разнообразных данных, полученных из различных источников: компьютеров и устройств, используемых преступниками для работы с криптовалютами.

Также, при расследовании таких преступлений требуется использование специализированных инструментов и программного обеспечения, которые могут помочь в анализе данных по криптокошелькам и биржам, транзакциям и создании пользовательских профилей.

Наконец, для расследования указанных преступлений важно тесно сотрудничать с экспертами из других сфер, таких как кибербезопасность, аналитика и финансы. Только вместе с этими специалистами можно достичь максимальной эффективности при их расследовании.

Несмотря на наличие правовой базы, которая только формируется и правовых возможностей изъятия криптовалюты, существуют как законодательные (хранение), так и организационные проблемы (обнаружение, идентификация).

Первое. Действующее законодательство относит криптовалюту к цифровым активам (Закон Республики Казахстан от 24.11.2015 года № 418-V ЗРК «Об информатизации»).

Гражданский кодекс Республики Казахстан содержит норму о цифровых активах (ст. 115 ч.2), согласно которой он относит их к имущественным благам и правам (имуществу) [5].

Уголовно-процессуальное законодательство предусматривает нормы касательно ареста и изъятия имущества [6].

Однако, в Правилах изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, утвержденных 09.12.2014г. постановлением Правительства Республики Казахстан №1291 отсутствуют нормы о порядке обращений с цифровыми активами [7].

В соответствии со статьей 33-1 Закона Республики Казахстан «Об информатизации», цифровые активы могут быть обеспеченными или необеспеченными. Выпуск и оборот необеспеченных цифровых активов на территории Республики Казахстан запрещаются, за исключением случаев, предусмотренных законами Республики Казахстан

(разрешается в рамках работы Международного финансового центра «Астана» (далее - МФЦА), но при условии полной идентификации) [8].

Вместе с тем, биткойн и другие виртуальные валюты, используемые преступниками, ничем не обеспечены и сильно волатильны.

Лица, занимающиеся противоправной деятельностью, никогда не пойдут в МФЦА, так как их главная цель скрыть свои доходы и свою личность в интернете.

Второе. Орган расследования сталкивается с организационными проблемами, а именно: с обнаружением и арестом криптовалют, идентификацией криптокошелька, конфискацией виртуальной валюты и обращением ее в доход государства.

Идентификация криптокошелька – следователь или оперативный сотрудник не знает, как привязать криптокошелек к конкретному лицу, потому, что при их регистрации не требуются паспортные данные.

Конфискация виртуальной валюты с криптокошельков – преступники добровольно не выдают приватный ключ (пароль), криптокошельки зарегистрированы в иностранных юрисдикциях.

Хранение криптовалюты – не во всех правоохранительных органах имеются ведомственные криптокошельки для хранения виртуальной валюты.

Более того, есть и другие проблемные вопросы, связанные именно с хранением виртуальной валюты в криптокошельках, по которым правоохранительным органам необходимо принять решение:

1) В правоохранительном органе будет один криптокошелек или несколько? Если один, то пароль и логин от него должен храниться у всех следователей, а это повышает риск утечки или хищение логина и пароля. В случае кражи биткоинов, будут трудности в установлении виновных лиц. Если несколько криптокошельков, то кто должен вести их учет в правоохранительном органе, кто будет являться ответственным лицом по формированию логина и пароля от него. Может ли один следователь иметь несколько криптокошельков? Должен ли следователь сообщать руководителю данные от криптокошельков (в случае его увольнения, он может изменить пароль и подменить находящиеся в нем криптовалюты). Если будут изъяты разные криптовалюты, но по одному уголовному делу, следователь должен создавать под каждую из них криптокошельки. Кто это будет делать, следователь или сотрудники, отвечающие за информационную безопасность?

Если несколько уголовных дел, по которым необходимо изъять биткоины, они должны храниться в одном криптокошельке или разных? Если в разных, то кто будет являться их ответственным лицом / администратором (управлять ими и обеспечивать безопасность).

2) Какой орган должен вести учет всех изъятых виртуальных валют по всем правоохранительным органам? Каждый орган самостоятельно или это должен делать КПСиСУ ГП РК?

Обращение криптовалюты в доход государства – нет инструкции, единого стандарта или регламента работы по виртуальной валюте.

Все эти вышеуказанные проблемы связаны с технологией блокчейн, которая обеспечивает безопасность, конфиденциальность и анонимность.

Несмотря на то, что в теории все транзакции на блокчейне являются открытыми, их анонимность делает их недоступными для обнаружения правоохранительными органами.

В будущем к числу вышеуказанных проблем может добавиться еще одна проблема, связанная с возвратом криптовалюты ее законному владельцу (имеются риски, связанные с возмещением государством понесенных владельцем криптовалюты потерь и материального ущерба).

Рассмотрим 3 варианта исхода дел, связанных с возвратом криптовалюты ее законному владельцу.

Вариант 1. Следователь по уголовному делу изъял криптовалюту (10 биткоинов), поместил ее в ведомственный криптокошелек, но в процессе расследования не смог доказать вину лица, у которого он их изъял (потеря электронных доказательств или признание судом их недопустимыми), он должен вернуть виртуальную валюту законному владельцу.

Однако на момент возврата криптовалюты ее стоимость на рынке существенно упала с 20 000 до 5 000 долларов США. Разница в 15 000 долларов США может стать предметом гражданского иска о возмещении материального ущерба и упущенной выгоды от несвоевременной продажи криптовалюты.

Бремя возврата денег ляжет на государство, которое должно изыскать средства в сумме 15 000 долларов США, но только в тенге по курсу на момент принятия решения о возврате и передать владельцу криптовалюты.

Вариант 2. Следователь по уголовному делу изъял криптовалюту (10 биткоинов), поместил ее в ведомственный криптокошелек, но в процессе расследования не смог доказать вину лица, у которого он их изъял, он должен вернуть виртуальную валюту законному владельцу.

Однако, вследствие утечки данных или просто целенаправленной хакерской атаки, криптовалюта будет похищена с виртуального кошелька правоохранительного органа. Как будут восстанавливаться биткоины или другие виртуальные валюты, если на такие цели бюджетные деньги не закладываются? Опять наши суды получат гражданские иски к таким правоохранительным органам.

Вариант 3. Следователь по уголовному делу изъял криптовалюту (10 биткоинов), по своему постановлению обменял ее на криптобирже в тенге (по цене 20 тыс. долларов за 1 биткоин) и разместил уже полученную сумму на специальный счет правоохранительного органа (предположим 93 млн. тенге = 10 биткоинов умножаем на 20 тыс. долларов и умножаем на курс тенге к доллару).

В процессе расследования не смог доказать вину лица, у которого он их изъял и по своему постановлению должен вернуть ему криптовалюту. Но на момент возврата ее стоимость существенно выросла и составляла уже не 20 000 долларов за 1 биткоин, а 50 000 долларов.

В итоге государство должно вернуть владельцу криптовалюты уже не первоначальную сумму (93 млн. тенге), а 232 500 000 тенге (50 тыс. долларов умножаем на 10 биткоинов и умножаем на курс тенге к доллару).

Для решения вышеуказанных проблем требуется тщательное изучение вопроса ареста, конфискации и хранения криптовалюты.

Заключение. Существует несколько подходов, которые можно использовать для борьбы с проблемой обнаружения, ареста и изъятия криптовалют. Одним из подходов является введение дополнительных регулирований в криптоиндустрии.

Регулирование - это особым образом, созданные правила и законы, которые устанавливаются для использования криптовалют. Существует несколько способов регулирования использования криптоактивов, но они сводятся к обязательной регистрации, легализации, проверке на соответствие стандартам безопасности, установления ограничений для использования криптовалют и применение налогов на использование этих цифровых активов.

Например, можно ввести обязательное лицензирование криптобирж и других криптовалютных компаний. Это позволит государству и правоохранительным органам больше контролировать данную сферу и легко отслеживать потоки криптовалют на таких биржах и других платежных платформах.

Еще одним подходом является улучшение сотрудничества:

- между правоохранительными органами и криптовалютными компаниями, которые могут предоставить им необходимую информацию о транзакциях и клиентах, что могло бы помочь в обнаружении и изъятии криптовалют;

- между правоохранительными органами и компаниями по безопасности и консалтингу, которые могут помочь им в борьбе с криптовалютными преступлениями за счет обучения и предоставления экспертной поддержки в сфере криптовалют.

- между правоохранительными органами Казахстана и другими государствами (такой подход может значительно увеличить

эффективность борьбы с преступлениями, связанными с криптовалютами).

Необходимо принимать и другие меры, такие как:

- разработка технологий и программного обеспечения по созданию более безопасной экосистемы для обмена криптовалют и подтверждения легитимности транзакций;
- создание образовательных программ по безопасности использования криптовалют и их отслеживанию.

Эти и другие меры позволят правоохранительным органам сосредоточиться на борьбе с криптопреступностью и повышении уровня безопасности криптовалютного пространства.

Список использованных источников:

1. Криптовалюты и блокчейн, как атрибуты новой экономики. Брошюра «Евразийская экономическая комиссия», Москва, 2019. – С. 7;
2. Возможности и перспективы развития криптовалют. Журнал «Международный студенческий научный вестник» - 2015. - № 4 (часть 3) – С. 433-436.
3. Получение взятки криптовалютой: вопросы квалификации. Журнал «Союз криминалистов и криминологов». – 2020. № 2 С. 19-25.
4. Блокчейн: Схема новой экономики / Мелани Свон: - Москва: Издательство «Олимп-Бизнес», 2017. – 240с.
5. Гражданский кодекс Республики Казахстан от 27 декабря 1994 года // [Электронный ресурс] – Режим доступа: http://10.61.42.188/rus/docs/K940001000_ (дата обращения 25.04.2023).
6. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК // [Электронный ресурс] – Режим доступа: http://10.61.42.188/rus/docs/K1400000231 (дата обращения: 25.04.2023).
7. Постановление Правительства Республики Казахстан от 09.12.2014 года №1291 «Об утверждении Правил изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, изъятых документов, денег в национальной и иностранной валюте, наркотических средств, психотропных веществ по уголовным делам судом, органами прокуратуры, уголовного преследования и судебной экспертизы» // [Электронный ресурс] – Режим доступа: http://10.61.42.188/rus/docs/P1400001291 (дата обращения: 25.04.2023).
8. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК // [Электронный ресурс] – Режим доступа: http://10.61.42.188/rus/docs/Z1500000418 (дата обращения: 25.04.2023).

УДК 004.8:343.98

Ким Клара Васильевна
Professor Emeritus Департамента уголовного правосудия
Высшей школы права KAZGUU, к.ю.н, доцент,
г. Астана, Республика Казахстан

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЗАДАЧИ КРИМИНАЛИСТИКИ

Аннотация. В статье рассматриваются вопросы дальнейшего совершенствования криминалистики в современных условиях развития цифровой экономики, необходимыми направлениями которого выступает формирование инновационных учений и теорий, обеспечивающих результативное обнаружение, исследование, фиксацию, оценку и использование криминалистической информации разной природы и формы в процессе раскрытия, расследования и предупреждении уголовных правонарушений. Рассмотрены вопросы истории становления теории цифровой криминалистики (криминалистической кибернетики). Автором обосновывается необходимость дальнейшего развития, в первую очередь, таких криминалистических учений, как криминалистическая классификация преступления, криминалистическая характеристика, следственные ситуации, тактические операции, криминалистическое исследование личности преступника, криминалистическая виктимология, представляющимися обязательными элементами методологической базы дальнейшей цифровизации криминалистики и использования ею возможностей искусственного интеллекта.

Ключевые слова: цифровая криминалистика; методы и методология криминалистики; частные криминалистические учения и теории; задачи криминалистики; информация; цифровые доказательства; цифровые следы; криминалистическое мышление; искусственный интеллект; алгоритмизация и программирование (не встречается в тексте) процесса расследования.

Аннотация. Мақалада цифрлық экономиканы дамытудың қазіргі жағдайында криминалистиканы одан әрі жетілдіру мәселелері қарастырылады, оның қажетті бағыттары қылмыстық құқық бұзушылықтарды ашу, тергеу және алдын алу процесінде әртүрлі сипаттағы және нысандағы криминалистикалық ақпаратты нәтижелі табуды, зерттеуді, бекітуді, бағалауды және пайдалануды қамтамасыз ететін инновациялық ілімдер мен теорияларды қалыптастыру болып табылады. Цифрлық криминалистика (криминалистикалық кибернетика) теориясының қалыптасу тарихы мәселелері қаралды. Автор, ең алдымен, қылмыстың криминалистикалық классификациясы, криминалистикалық сипаттамасы, тергеу жағдайлары, тактикалық операциялар, қылмыскердің жеке басын криминалистикалық зерттеу, криминалистикалық виктимология сияқты криминалистикалық ілімдерді одан әрі дамыту қажеттілігін негіздейді, олар криминалистиканы одан әрі цифрландырудың және оның жасанды интеллект мүмкіндіктерін пайдаланудың әдіснамалық базасының міндетті элементтері болып табылады.

Түйінді сөздер: сандық криминалистика; криминалистиканың әдістері мен әдістемесі; жеке криминалистикалық ілімдер мен теориялар; криминалистиканың міндеттері; ақпарат; цифрлық дәлелдер; цифрлық іздер; криминалистикалық ойлау; жасанды интеллект; алгоритмдеу және тергеу процесін бағдарламалау.

Annotation. The article discusses the issues of further improvement of criminalistics in the modern conditions of the digital economy development, the necessary directions of which are the formation of innovative doctrines and theories that ensure the effective detection, research, fixation, evaluation and use of forensic information of different nature and form in the process of disclosure, investigation and prevention of criminal offenses. The issues of the history of the formation of the theory of digital criminalistics (forensic cybernetics) are considered. The author substantiates the need for further development, first of all, of such criminalistic exercises as criminalistic classification of crime, criminalistic characteristics, investigative situations, tactical operations, criminalistic investigation of the criminal's personality, criminalistic victimology, which are mandatory elements of the methodological basis for further digitalization of criminalistics and its use of artificial intelligence capabilities.

Keywords: digital criminalistics; methods and methodology of criminalistics; private forensic studies and theories; tasks of criminalistics; information; digital evidence; digital traces; forensic thinking; artificial intelligence and programming of the investigation process.

В современном мире наступление цифровой эпохи обусловливает успешность экономической, политической, социальной и духовной сферах деятельности, в первую очередь, использованием для достижения своих задач методов и положений информационных технологий.

В области юридических наук одной из первой, поставившей проблему о необходимости активного и творческого использования кибернетических и математических методов, стала криминалистика. В 1982 году, в то время доцент кафедры криминалистики МГУ им. М.В. Ломоносова, Н.С. Полевой опубликовал учебное пособие по новому спецкурсу – «Криминалистическая кибернетика» [1], где отметил, что основой кардинальных изменений, происходящих в производственной и научной деятельностях, являются «процессы активного использования математических методов, средств автоматизации, вычислительной техники, идей и методов кибернетики и связанных с ней наук» [1, с. 3]. Данный подход позволяет «глубже проникать в сущность изучаемого явления или процесса, всесторонне познать не только элементы изучаемого явления, но и функции всей системы как целостного образования» [1, с. 4]. В 1973 году Н.С. Полевым также предложен спецкурс по криминалистической кибернетике, который преподавался на юридическом факультете МГУ им. М.В Ломоносова.

Профессор Н.С. Полевой в своем труде «Криминалистическая кибернетика» поставил целый ряд вопросов и проблем, которые заложили основу не только для её становления, как частной криминалистической теории, но и дальнейшего её развития (компьютерная криминалистика, цифровая криминалистика). Николай Степанович Полевой по праву является первооткрывателем нового научного направления (научного прогресса), частной криминалистической теории – криминалистической кибернетики,

заложившим её методологические основы и определившим обязательные направления совершенствования науки криминалистики.

Выделяя в качестве объекта криминалистической кибернетики деятельность по использованию кибернетических методов и положений, он подчеркивал комплексный характер учения и необходимость привлечения знаний равно как правовых, так и из сферы компьютерных технологий. С учетом самостоятельности данных научных отраслей, их специфики, сложности, оптимальной и результативной формой развития деятельности по использованию кибернетических методов представляется взаимодействие представителей данных двух специальностей.

Такое взаимодействие как согласованная деятельность, ориентированная на решение общей задачи, позволяет применить возможности обеих наук: положения криминалистических учений и теорий, направленных на достижение сформулированных перед ней задач, и возможностей их решения с помощью компьютерных (информационных) технологий. Ярким примером такого взаимодействия может служить использование научных положений учения об идентификации лица по внешним признакам и информационных технологий для оперативного установления личности по графическому распознаванию лица на основе его изображений, имеющихся в социальных сетях, в других базах интернета (нейросети). В настоящее время графическое распознавание лица широко используется в самых различных сферах жизни человека, где необходима его идентификация по внешним признакам – разблокировке телефона, при входе в учреждение, аэропортах, банках и т.д. Первыми заказчиками и пользователями единой биометрической системы, которая позволяет идентифицировать человека по его биометрическим характеристикам, закономерно стали банки, которые ставили задачи повышения безопасности финансовых операций своих клиентов и их идентификацию. В практической деятельности правоохранительных органов графическая идентификация применяется в уголовной регистрации, а также в судебно-экспертной практике. Развитие данного направления с привлечением нейросетей предполагает быстрое решение не только идентификационной задачи личности, но и установление его настоящего места нахождения, практически в любой точке земного шара. Однако, такая деятельность обусловливает определение правовых и нравственных оснований для их применения с учетом законных прав и интересов человека как объекта подобных действий. Теоретико-методологическими основами графической идентификации личности послужило использование научных положений об индивидуальности, устойчивости, восстанавливаемости, многообразии внешних признаков человека, обеспечивающие достоверность её результатов. На основе выявления

идентификационных свойств внешних признаков человека основатель криминалистического учения о них, Альфонс Бертильон [2], ещё в 80-ых года XIX века предложил правила сигналетической съемки, словесного портрета, антропометрической идентификации, использование которых претерпели радикальные результативные изменения с применением информационных технологий.

Развитие цифровой криминалистики предполагает правильное определение её содержательной структуры и методологических основ. Формирование структуры частного криминалистического учения обусловливается особенностями самой криминалистической науки, её объектом, системой и задачами.

Зарождение криминалистики как самостоятельной науки было обусловлено целым рядом факторов, отразивших особенности борьбы с преступностью в начале - середине 20 века. В условиях научно-технической революции, промышленного прогресса, урбанизации городов, демократизации уголовного судопроизводства, качественно изменилась и преступность, отразившая особенности новой эпохи, повысив свой профессиональный и организационный уровень [3, с.1-2]. Задача формирования системы эффективных методов раскрытия, расследования и предупреждения различного рода преступлений не могла разрабатываться в рамках традиционных отраслевых правовых наук уголовного цикла, поскольку выходила за пределы их компетенций.

Искусство расследования формировалось отдельными практиками раскрытия преступлений и учеными-исследователями, старавшимися использовать результаты научных открытий того времени в медицине, химии, физике, психологии, психиатрии, баллистике, графологии, антропометрии, дактилоскопии, логике, фотографии, микроскопии, ботанике, а также использовать обобщенный опыт ведения уголовных дел и изобличения преступников, их язык (воровской жаргон) и особенности отношений. Такой подход качественно расширял возможности детективов в поисках следов совершенного преступления, их исследования с целью получения заключенной в ней информации, фиксации в протоколе и с помощью технических средств, обеспечивающих их достоверность.

В 1892 году судебный следователь из Черновцов Ганс Гросс, имевший более 20 летний следственный стаж, на основе анализа накопленного опыта раскрытия преступлений и практики внедрения в расследование положений и методов, бурно развивавшихся в тот период наук, издает «Руководство для судебных следователей, чинов общей и жандармской полиции». В 1898 году данный труд переиздается под названием «Руководство для судебных следователей как система криминалистики» [4, с.N-O]. Он стал первым учебником по криминалистике. Ганс Гросс «сумел показать громадное значение научного приспособления данных других наук для расследования

преступлений и тем самым создал науку криминалистику» [5, с.68]. Будучи специфической правовой дисциплиной, направленной на успешное достижение задач, закрепленных в уголовном и уголовно-процессуальных кодексах, криминалистика обладает собственными задачи и отличительными свойствами. К таким свойствам следует отнести правовой, комплексный и прикладной характер криминалистики, доминирующим методом которой является анализ судебно-следственной и экспертной практики. Если благодаря активному творческому приспособлению данных других наук к требованиям отправления правосудия по уголовным делам способствовало появление криминалистики в качестве самостоятельной дисциплины и стало её отличительной особенностью [6, с.71], то и дальнейшее её развитие и прогнозирование должно осуществляться в соответствии данным же свойством вкупе с другими. «Развитие и специализация естественнонаучного знания в криминалистике идёт не по пути выделения автономных частнонаучных комплексов, а по пути формирования внутри криминалистики и, что самое главное, на базе её теории и методологии специализированных направлений, обеспечивающих решение типовых криминалистических задач применительно к типовым криминалистическим объектам» [7, с. 14].

Система криминалистики в соответствие с поставленными перед ней задачами строилась по структуре её объекта. В настоящее время в отечественной криминалистике и стран СНГ под объектом криминалистики понимается двуединый: с одной стороны - деятельность преступная, с другой стороны – деятельность по расследованию преступлений. Однако, данные объекты являются общими для многих правовых дисциплин, в то время как изучаются они для решения несовпадающих между собой задач, что и отличает их предмет.

Прикладной характер криминалистики определен главным вопросом, сформированным социальной потребностью - разработка рекомендации по применению средств, приемов, методик по результативному, эффективному раскрытию, расследованию преступлений. Данный главный вопрос получил отражение в частных задачах криминалистики – обнаружение, исследование, фиксация, изъятие, оценка и использование криминалистической информации и её источников. С учетом природы криминалистической информации, её источников и механизма их образования построена традиционная система криминалистики, состоящая из четырех разделов: общая науковедческая часть, криминалистические техника, тактика и методика. Она отражает предметные срезы единого объекта криминалистики, соответствующие её задачам: работа с материальными источниками, работа с идеальными источниками, работа с данными видами источников (следов) с учетом механизма их образования по отдельным криминалистическим видам преступлений и ситуаций.

Возникает вопрос о соотношении структуры цифровой криминалистики с основной дисциплиной (наукой) криминалистикой.

Под криминалистической кибернетикой Полевой Н.С. понимал частную криминалистическую теорию, являющуюся комплексной отраслью знания об общих закономерностях и конкретных методах математизации и автоматизации информационных процессов в сфере деятельности по раскрытию и расследованию преступлений, разрабатываемых и используемых в целях её оптимизации и повышения эффективности функционирования как кибернетической системы [1, с 15-16]. Особое значение научных исследований Н.С. Полевого заключается, на наш взгляд, в методологии подхода к необходимости формирования нового комплексного направления в криминалистической деятельности на основе привлечения новых научных методов, расширяющих познавательные возможности криминалистической деятельности и соответственно новых источников полезной и необходимой для расследования информации (математической, цифровой).

Потребности побуждают деятельность и управляют ею со стороны субъекта, но способны выполнять эти функции при условии, что они являются предметными [8]. Профессор Н.П. Яблоков подчеркнул закономерную взаимосвязанность развития и расширения представлений об объекте исследованиями и достижениями научно-технической революции [9, 89]. С одной стороны, любая деятельность предметна, с другой стороны, - активное и творческое использование данных других наук не только являются одним из факторов, обусловивших появление криминалистической науки, но также и её дальнейшее развитие. В этом аспекте можно свидетельствовать не только о новых методах, используемых в деятельности по раскрытию, расследованию и предупреждению уголовных правонарушений, но и открывшимся благодаря данным методам и средствам, возможностям исследовать иные по природе источники криминалистической информации, в данном случае – цифровые. Таким образом, предметные срезы в едином объекте криминалистике – деятельности: преступной и криминалистической, расширяются. Данное положение является одной из предпосылок возникновения и создания новых или развития криминалистических учений и теорий.

В настоящее время, через тридцать лет после появления работы Н.С. Полевого о криминалистической кибернетике, решение многих задач в области уголовного судопроизводства непосредственно связано с применением компьютерных технологий: методики различных видов экспертного исследования; система криминалистического обеспечения расследования; организация уголовной регистрации; работа с цифровыми источниками информации; электронное судопроизводство;

организация деятельности правоохранительных органов, их взаимодействие и др.

Закономерно, что встает вопрос о подготовке специалиста новой отрасли знаний, обладающего «компетенциями в области криминалистики, а также судебных компьютерно-технических исследований и экспертиз» [10, с.8]. В условиях давно назревшей потребности в учебнике, направленном на подготовку компетентных специалистов, владеющими не только юридическими, но и знаниями, методами информационных технологий, умеющими их применять в криминалистических ситуациях расследования, вышедший в 2022 году труд под редакцией д.ю.н. В.Б Вехова и д.ю.н. С.В. Зуева «Цифровая криминалистика», представляется этапным событием в развитии криминалистической науки. В настоящем учебнике получили отражение современный уровень криминалистической науки, анализирована практика использования инновационных технологий в процессе обнаружения исследования, фиксации и оценки источников криминалистической информации, в то числе и цифровой.

В работе обоснованы теоретические и методологические основы формирования новой частной криминалистической теории, на основе структурной связи объекта и предмета криминалистики, её системы и задач определены система, объект и предмет цифровой криминалистики. Под цифровой криминалистикой понимается «частная криминалистическая теория, которая представляет собой систему научных положений и разрабатываемых на их основе технических средств, приемов методик и рекомендаций по обнаружению, предварительному исследованию, использованию компьютерной информации и средств её обработки в целях раскрытия, расследования и предупреждения преступлений» [10, с.25]. Исходя из понимания предмета исследования цифровой криминалистики с учетом содержания её основных функций – познавательной и конструктивной, предложена структура данного частного учения.

Таким образом, в систему цифровой криминалистики включены разделы, связанные с появлением новых источников криминалистической информации – цифровых и особенностями работы с ними – поиска, обнаружения, исследования, фиксации, изъятия, использования с целью получения доказательств по уголовному делу.

Самостоятельного рассмотрения требуют и носители цифровой информации (компьютерные, цифровые устройства), работа с которыми требует привлечения специалиста. Особенности данного объекта исследования ставят вопрос о процессуальном, организационном и тактическом обеспечении следственных действий, направленных на работу с ними с целью получения доказательств. Возможности информационных методов позволяют их использовать для

эффективного решения прикладных задач организационного, тактического и методического характера.

Дальнейшее развитие цифровой криминалистики связано с возможностями создания искусственного интеллекта в виде двойника-криминалиста или конструктивной функцией.

«Цифровой образовательный двойник осуществляет генерацию разнообразных умных данных (Smart Big Data.), получаемых в результате многоаспектного осуществления образовательного процесса, включая формирование сетевых образовательных способностей и профессиональных компетенций обучаемых, которые могут быть использованы для моделирования сценариев поведения, функционирования и развития, как всего образовательного процесса, так и отдельных его элементов» [11].

В основе умных данных для принятия криминалистических решений должны будут находиться те, которые отражаются в рекомендации по их принятию в конкретных ситуациях расследования отдельных видов уголовных правонарушений. Поэтому основной базой генерируемых данных должны стать положения и рекомендации таких частных криминалистических учений и теорий, как криминалистическая классификация преступлений, теория криминалистической характеристики, учение о следственных версиях и моделировании, учение о следственных ситуациях, учение о тактических рисках, частные криминалистические методики. В первую очередь, на наш взгляд, данные положения определяют основу криминалистического мышления [12].

При этом отдельной проблемой будут вопросы, связанные с правовыми и нравственными пределами функционирования двойников-криминалистов в уголовном судопроизводстве.

Список использованных источников:

1. Полевой Н.С. Криминалистическая кибернетика. – М.: Изд-во МГУ, 1982. – 208 с.
2. Юргенс Торвальд. Сто лет криминалистики. М.: Прогресс, 1975. – 448 с.;
3. Криминалистика. Учебник для вузов. Под редакцией профессора Р.С. Белкина. – М.: НОРМА-ИНФРА М, 1999.- 990 с.
4. Гросс Г. Руководство для судебных следователей как система криминалистики. – Новое изд., переч.с изд. 1908 г. – М.: ЛексЭст, 2002. – 1088 с.
5. Шавер Б.М. Предмет и метод советской криминалистики // Соц.законность, 1938, № 6.
6. Величкин С.А. Научные основы криминалистики // Вестник Санкт-Петербургского университета. Право. 2013, № 14. Вып. 3. – С. 65-99.
7. Колдин В.Я. Естественно-научная криминалистика в системе современного криминалистического знания. Вступительная статья // Клаус Дитер Поль. Естестенно-научная криминалистика (Опыт применения научно-технических средств при расследовании отдельных видов преступлений). - М.: Юрид. лит-ра, 1985.- 304 с.

8. Леонтьев А.Н. Деятельность. Сознание. Личность. / А.Н. Леонтьев. - 2-е изд. - Москва: Политиздат, 1977. - 304 с.

9. Яблоков Н.П. К вопросу о криминалистическом мышлении // Правовые проблемы укрепления российского государства. – Сб. статей. Томск, 2012 – С. 156-159)

10. Цифровая криминалистика: учебник для вузов/ В.Б. Вехов [и др.]; под редакцией В.Б. Вехова, С.Н. Зуева. – М.: Изд-во Юрайт, 2022. – 417 с.

11. Цифровые образовательные двойники и искусственный интеллект как драйверы развития гиперконкурентной нейро-сетевой экономики/ Экспертное заключение подготовлено по итогам сессии ПМЭФ-2022 «Цифровой след: заявка на будущее». Автор: Дятлов Сергей Алексеевич, д.э.н. [Электронный ресурс] // Режим доступа: https://roscongress.org/materials/tsifrovye-obrazovatelnye-dvoyniki-i-iskusstvennyy-intellekt-kak-drayvery-razvitiya-giperkonkurentnoy / (дата обращения: 03.05.2023 г.)

12. Бахтеев Д.В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений Автореферат дисс. на соиск. учён. степени д-ра юрид. наук. Екатеринбург – 2022. [Электронный ресурс] // Режим доступа: https://www.dissercat.com/content/kontseptualnye-osnovy-teorii-kriminalisticheskogo-myshleniya-i-ispolzovaniya-sistem-iskusstv (дата обращения: 03.05.2023 г.).

УДК 343.98:004.8

Климова Яна Александровна
Доцент кафедры криминалистики учебно-научного комплекса
по предварительному следствию в ОВД
Волгоградской академии МВД России,
кандидат юридических наук,
г. Волгоград, Российская Федерация

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ИНСТРУМЕНТ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

Аннотация. В течение нескольких последних лет неизменно высокими остаются показатели совершения преступлений с использованием информационно-телекоммуникационных технологий. Важное значение для эффективного расследования рассматриваемых преступлений имеет качественное производство предварительного расследования. Автором делается вывод о целесообразности интеграции современных технологий в процесс расследования преступлений в условиях цифровизации, в том числе технологии искусственного интеллекта, нейросетей.

Ключевые слова: искусственный интеллект; нейросети; цифровая криминалистика; информационные технологии; преступления с использованием информационно-телекоммуникационных технологий; цифровизация; интеграция технологий.

Аннотация. Соңғы бірнеше жылда ақпараттық-телекоммуникациялық технологияларды қолдану арқылы жасалған қылмыстар деңгейі тұрақты түрде жоғары болып қалды. Қаралып отырған қылмыстарды тиімді тергеу үшін алдын ала тергеудің сапасы маңызды. Цифрландыру жағдайында қылмыстарды тергеу процесіне заманауи технологияларды, оның ішінде жасанды интеллект технологиялары мен нейрондық желілерді енгізудің орындылығы туралы қорытынды жасалды.

Түйінді сөздер: жасанды интеллект; нейрондық желілер; сандық криминалистика; ақпараттық технологиялар; ақпараттық және телекоммуникациялық технологияларды пайдаланатын қылмыстар; цифрландыру; технологияларды біріктіру.

Annotation. Over the past few years, the rates of crimes committed using information and telecommunication technologies have remained consistently high. The quality of the preliminary investigation is essential for the effective investigation of the crimes under consideration. The conclusion is made about the expediency of integrating modern technologies into the process of investigating crimes in the context of digitalization, including artificial intelligence technologies and neural networks.

Keywords: artificial intelligence; neural networks; digital forensics; information technology; crimes using information and telecommunication technologies; digitalization; technology integration.

В настоящее время одним из мировых трендов современности является стремительное развитие различных информационно-телекоммуникационных технологий, цифровизация всех сфер жизни.

Эта тенденция оказывает влияние и на картину преступности. Все большее количество преступлений можно отнести к категории высокотехнологичных. Даже «традиционные» преступления сегодня совершаются с использованием информационно-телекоммуникационных технологий.

Согласно статистическим данным в январе - феврале 2023 года в России зарегистрировано 93,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 17,1% больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 26,3% в январе - феврале 2022 года до 30,6%.

Анализ данных позволяет выделить наиболее популярные способы совершения таких преступлений:

- три четверти (75,1%) совершается с использованием сети «Интернет» (70,1 тыс.; +24,1%);
- почти половина (42,2%) совершается с использованием средств мобильной связи (39,4 тыс.; +17,3%);
- более чем две трети таких преступлений (69,6%) совершается путемкражи или мошенничества: 64,9 тыс. (+6,7%);
- каждое седьмое (14,2%) – с целью незаконного производства, сбыта или пересылки наркотическихсредств: 13,3 тыс. (+69,3%) [1].

Данные статистики свидетельствуют об актуальности исследования современных способов раскрытия и расследования высокотехнологичных преступлений.

Наиболее перспективным направлением, позволяющим эффективно и качественно раскрывать и расследовать указанные преступления, является использование возможностей искусственного интеллекта как инструмента цифровой криминалистики. Следует обратить внимание, что различные IT-технологий, и в частности искусственный интеллект, разрабатываются на протяжении последних нескольких лет и в предыдущем году этот сегмент стал одним из самых инвестируемых направлений. Однако актуальность нашего исследования обуславливается еще и тем, что технологии искусственного интеллекта в последнее время все чаще попадает в сферу внимания законодателя и ученых-криминалистов [2].

В настоящий момент существенной проблемой использования искусственного интеллекта при расследовании преступлений является наличие правовых лакун, регулирующих указанную сферу, отсутствие соответствующей нормативно-правовой базы, этических норм. Решение данной проблемы видится нам в разработке и совершенствованию законодательной регламентации рассматриваемых общественных отношений.

Несмотря на это, следует отметить, что в настоящее время к средствам технико-криминалистического обеспечения цифровой

криминалистики, основанным на алгоритме искусственного интеллекта, которое уже может использовать специалист в ходе осмотра электронных носителей информации, относится программное обеспечение для компьютерно-технического исследования устройств («Мобильный Криминалист», «UFED», «BELKASOFT EVIDENCE CENTER» и другие). Такие программы позволяют извлекать криминалистически значимую информацию из мобильных устройств, ноутбуков, персональных компьютеров и облачных сервисов. Искусственный интеллект позволяет делать аналитику извлечений: строить графы связей, осуществлять распознавание лиц и текста, определять различные виды угроз (оружие, наркотики, терроризм, экстремизм и т.д.) и многое другое.

Перспективным направлением считаем интеграцию нейротехнологий в процесс расследования.

Под нейротехнологией в цифровой криминалистики предлагаем понимать как метод искусственного интеллекта, основанный на глубоком машинном обучении данных, направленный на изучение информации в целях раскрытия и расследования преступлений.

Полагаем, что позволит расширить горизонт расследования, применение следующих нейротехнологий:

1) Создание трехмерных сцен и 3D-панорамы из 2D-изображений. Модель может быстро обработать несколько десятков фотографий, приняв при этом в расчет ракурсы камеры, с которых велась съемка, и затем визуализировать получившуюся 3D-сцену (например, нейросеть NeRF, приложение Luma AI). В ходе расследования такая технология позволит создавать трехмерные модели участков местности, помещений, жилищ, транспортных средств, предметов, фотографирование которых осуществлялось в ходе производства следственных действий, таких как следственный осмотр, обыск, выемка, осмотр предметов и другие).

2) Редактирование людей на видео с функцией изменения эмоций, возраста, макияжа. Отличие от предыдущих методов в том, что для обработки одного кадра используются изменения, которые применяли в предыдущих (есть зависимость от времени) (например, генеративно-состязательная нейросеть (Generative adversarial network). Использование данной технологии позволит улучшать видео, полученное с камер видеонаблюдения, с целью установления личности либо идентификации лица, запечатленного на месте совершения преступления.

3) Кластеризация данных. Метод можно использовать для выявления закономерностей и связей, позволяющих устанавливать людей и группы, занимающихся преступной деятельностью(например, блокчейн-технологии, алгоритм DeepClaster).

Интересным примером может послужить зарубежный опыт в рассматриваемой сфере. Так, 29-летний мужчина из китайской провинции Фуцзянь в ходе конфликта задушил свою девушку. Чжан вспомнил, что у его девушки на банковском счете были большие деньги, и решил воспользоваться накоплениями. Убийца запустил банковское приложение «MoneyStation» и поднес смартфон к лицу мертвой, но алгоритмы отказались авторизовать его. Искусственный интеллект «заподозрил» неладное и попросил девушку подмигнуть, чего она естественно не сделала. В итоге убийца не смог снять деньги. Но на этом его неудачи не закончились. Программа зарегистрировала подозрительную попытку входа в систему, так как искусственный интеллект не смог найти признаков движения в глазах жертвы, и передала информацию в правоохранительные органы. Те вручную проверили данные, которые собрала программа, и увидели след от веревки на шее девушки, а также услышали вместо женского голоса мужской. До того как преступник успел сжечь тело девушки, полиция его задержала. Так искусственный интеллект помог раскрыть преступление [3].

Несмотря на весьма впечатляющие перспективы применения современных технологий, основанных на искусственном интеллекте, в том числе в процессе расследования преступлений, такое интенсивное развитие этой области вызывает беспокойство общества. Так, широкую известность приобрело открытое письмо, опубликованное 28 марта на сайте организации FutureofLife, подписано главой Tesla, SpaceX и TwitterИлономМаском, со основателем Apple Стивом Возняком, со основателем PinterestЭваном Шарпом. Также подписи под документом поставили более 1 тыс. экспертов в области разработок искусственного интеллекта. Речь в нем идет о необходимости приостановить тренировки мощных систем хотя бы на полгода [4].

Таким образом, интеграция технологии искусственного интеллекта в процесс расследований преступлений видится нам весьма перспективным направлением, требующим дальнейшего научного осмысления. При этом тщательной правовой регламентации требуют вопросы пределов применения, ограничений и требования по разработке рассматриваемой технологии в целях соблюдения прав и законных интересов человека и гражданина.

Список использованных источников:

1. Официальный сайт Министерства внутренних дел Российской Федерации. [Электронный ресурс] – Режим доступа: https:// мвд.рф/dejatelnost/statistics (дата обращения: 24.04.2023 г.).

2. Национальная стратегия развития искусственного интеллекта на период до 2030 года // Утв. Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». [Электронный ресурс] – Режим доступа: СПС «КонсультантПлюс» (дата обращения: 16.04.2023 г.).

3. South China Morning Post. URL: https://www.scmp.com/news/china/society/article/3023964/chinese-murder-suspect-caught-ai-software-spotted-dead-persons (датаобращения: 09.04.2023).
4. Официальный сайт «Газета «Известия». [Электронный ресурс] – Режим доступа: https://iz.ru/1490348/2023-03-29/sozdatelei-iskusstvennogo-intellekta-prizvali-ostanovit-razrabotki(дата обращения: 24.04.2023 г.).

УДК 347.91/.95

Константинов Павел Денисович
ассистент кафедры гражданского процесса Уральского государственного юридического университета им. В.Ф. Яковлева, кандидат юридических наук, доктор права Франции
г. Екатеринбург, Российская Федерация

ИЗНАЧАЛЬНЫЕ ПРОБЛЕМЫ ВНЕДРЕНИЯ СИСТЕМЫ ПРЕДИКТИВНОГО ПРАВОСУДИЯ В СУДЕБНУЮ СИСТЕМУ СТРАН РОМАНО-ГЕРМАНСКОЙ ПРАВОВОЙ СЕМЬИ

Аннотация. Предиктивное правосудие является высокорискованной цифровой технологией, которая основывается на слабом искусственном интеллекте [1; 137-138]. В данной статье проанализированы проблемы устранимого характера, которые способно вызвать внедрение в систему гражданского процесса предиктивное правосудие. В результате анализа отечественных и зарубежных подходов к использованию данных технологией была сделана выборка некоторых проблем, которые вызывает внедрение предиктивного правосудия в область гражданского процесса. В заключительной части автором приводятся некоторые выводы касательно возможного использования инструментов предиктивного правосудия.

Ключевые слова: гражданский процесс; цифровизация; цифровые технологии; искусственный интеллект; предиктивное правосудие; континентальное право.

Аннотация. Болжамдық әділеттілік – әлсіз жасанды интеллектке негізделген қауіптілігі жоғары цифрлық технология [1; 137-138]. Бұл мақалада азаматтық процесс жүйесіне болжамды сот төрелігін енгізу нәтижесінде туындауы мүмкін жойылатын сипаттағы мәселелер талданады. Деректерді технология бойынша пайдаланудың отандық және шетелдік тәсілдерін талдау нәтижесінде азаматтық іс жүргізу саласына болжамды сот төрелігін енгізуден туындаған кейбір мәселелерге іріктеу жүргізілді. Қорытынды бөлімде автор болжамды әділеттілік құралдарын қолдану мүмкіндігіне қатысты кейбір қорытындыларды ұсынады.

Түйінді сөздер: азаматтық процесс; цифрландыру; цифрлық технологиялар; жасанды интеллект; болжамды әділеттілік; континенттік құқық.

Annotation. Predictive justice is a high-risk digital technology that is based on weak artificial intelligence [1; 137-138]. This article analyzes the problems of avoidable character, which can cause the introduction of predictive justice into the system of civil proceedings. As a result of the analysis of domestic and foreign approaches to the use of these technologies, a sample of some of the problems caused by the introduction of predictive justice in the field of civil procedure was made. The author concludes with some conclusions about the possible use of predictive justice tools.

Keywords: civil procedure; digitalization; digital technology; artificial intelligence; predictive justice; continental law.

Введение. Среди всей панорамы существующих информационных технологий, бесспорно, особый интерес представляют цифровые

технологии, характерной особенностью которых является использование так называемого «слабого» искусственного интеллекта.

Внутри же этой системы стоит уделить пристальное внимание такой достаточно необычной технологии, как предиктивное правосудие. Наиболее обобщенная схема использования данной технологии выглядит следующим образом:

Предиктивное правосудие представляет собой набор алгоритмов, которые функционируют на основе больших данных судебных решений и, проводя обработку естественного языка, способны выдавать статистический процент разрешения спора в пользу той или иной стороны, а также средний процент компенсационных выплат. Если цитировать французского представителя данного программного обеспечения Predictice, таким образом, программное обеспечивает «возможность иметь нормативный голос тысячам судей» [2; 91].

Несмотря на достаточно ощутимое количество плюсов, которые несет это программное обеспечение (будь то преимущество времени, повышение эффективности правосудия, повышение доступности правосудия, небывалый уровень объективности при рассмотрении споров, предсказуемость права и проч.), стоит, тем не менее, обратить большое внимание на изначальные проблемы, связанные с внедрением системы предиктивного правосудия в судебную систему стран романо-германской правовой семьи.

Основная часть.

1. Ограниченность алгоритмов.

Было бы несправедливым сказать, что уже сейчас мы имеем дело с полностью автоматизированной системой, способной полностью рассматривать юридические споры. В первую очередь, конечно, это выражается в том, что алгоритм не имеет абстрактного мышления, что не позволяет ему в каждом конкретном случае трактовать неопределенные правовые понятия типа «вины», «доброй воли», «добросовестности» и прочее [3; 15, 4; 193].

Кроме того, не совсем будет понятно, каким образом формировать большие и открытые данные судебных решений. Чем больше решений будет положено в основу алгоритма, тем больше будет риск попадания в базу условно «плохих» судебных решений – то есть ложных прецедентов, искажения информации в результате цифровой обработки и проч. [5; 57]. Данный тезис тем более усугубляется тем фактом, что практика убеждающего значения в одночасье способна перечеркнуть существующие до этого подходы к разрешению определенных категорий дел. Выражаясь более поэтично, можно привести цитату Ю. фон Кирхмана, немецкого правоведа: три новых слова высшей судебной инстанции, и целый пласт судебной практики становится макулатурой [6; 26].

2. Посредственная необъективность машины

В противовес сторонникам предиктивного правосудия, которые обосновывают преимущества этого алгоритма небывалым уровнем объективности машины при рассмотрении споров [2; 91, 7, 8; 118-120], критики приводят, кажется, уже ставший хрестоматийным пример программного обеспечения COMPAS, в ходе функционирования которого были выявлены предрассудки в отношении темнокожего населения. Эти предрассудки были отражены в программном коде алгоритма [9; 33, 10; 83].

На наш взгляд, суть данной проблемы кроется в том, что архитектором данного программного обеспечения выступает программист, который зачастую не имеет юридического образования и, в силу своей специализации, не всегда может обращать внимание на такие чисто юридические аспекты. Ключом к решению этой проблемы выступает, конечно, совместная работа юристов и программистов, а также выход в междисциплинарную модель обучения [11; 61]. В этой связи особо показательным является широко употребляемая во французской юридической литературе цитата C. O'Neil «Алгортим – это мнение, формализованное в коде» [12; 53-54].

3. Неконтролируемость машины

Главный вопрос, который описывает весь этот блок – сможет ли судья повлиять на решение машины?

Статистические данные судебной практики в России и Франции показывают, что судьи оказывают огромное, чуть ли не безоговорочное доверие экспертным заключениям [12; 48]. Можно привести аналогию с предиктивным правосудием – субъекту предоставляются вопросы, на которые он, с учетом специальных знаний, неизвестных судье, отвечает, а судья эти ответы принимает.

Модель функционирования алгоритмов предиктивного правосудия является непрозрачной, то есть непонятной любому юристу (что зачастую в научной литературе называют «черным ящиком»), не имеющему технических знаний, что может привести к тому, что результат сложного расчета будет для судьи единственной основой, а функции судьи трансформируются в простое визирование документов. Фактически существует достаточно большой риск нарушения гарантий реализации принципа независимости судей. Кроме того, если следовать мысли A. Garapon и J. Lassègue, широкое внедрение цифровых технологий в область правосудия приводит к росту цифровой неграмотности как со стороны обычного человека, который обращается в суд за защитой своих интересов, так и со стороны юристов, которые будут разрешать возникшие споры [13; 170]. Конечным итогом повышения цифровой неграмотности может стать снижение доверия к правосудию.

4. Инстанционность процесса

Судебная система России построена таким образом, что многоступенчатое обжалование судебных решений возможно в порядке ревизионного и чрезвычайного обжалования. Алгоритмы предиктивного правосудия рассматривают всю базу судебных решений и предлагают, на их основе, своё. Получается парадокс. Выходов из него может быть несколько:

• Алгоритмы необходимо разработать под все существующие в каждом правопорядке инстанции. Однако в таком случае мы закономерно придём к вопросу: какой смысл функционирования алгоритмов первой инстанции, если существуют «проверяющие», которые могут учитывать ошибки всех предыдущих инстанций? Нахождения в системе гражданского процесса нескольких алгоритмов разной степени качества, как нам кажется, в корне не соответствует цели оптимизации гражданского судопроизводства, но имеет и обратное действие. Необходимость постоянной вёрстки алгоритма первой инстанции вслед за отменой решения в инстанционном суде вызовет необходимость корректировки сразу всех алгоритмов. Организационные, финансовые и временные вопросы этой вёрстки, кажется, с лихвой могут перекрыть то темпоральное достоинство, которое выделяют сторонники предиктивного правосудия.

- Алгоритм будет единым. При более детальном погружении мы обнаружим, что различных случаев несколько:

o Алгоритм будет единым вообще для всех судов. В таком случае закономерным будет вопрос – есть ли смысл, в таком случае, нахождения всех остальных инстанций? Но стоит ли сносить всю выстроенную систему гражданского производства в угоду алгоритма, не имеющего «сильного» искусственного интеллекта, но обладающего всеми негативными моментами, разобранными ранее? Вопрос носит весьма дискуссионный характер.

o Алгоритм будет применяться лишь на стадии рассмотрения дела в суде первой инстанции. Весь пересмотр будет сохраняться в руках человека. Концептуально данный вариант не выглядит плохим. Однако, при системном рассмотрении феномена предиктивного правосудия, мы отмечаем несколько элементов: потенциально негодные для обработки решения, имитирование юридических силлогизмов вместо установления причинно-следственной связи, чистая рациональность машины, незнание правил работы алгоритма – не позволят нам говорить, что судья апелляционного суда и выше смогут адекватно понять, какие аргументы или факты оказались для машины решающими для принятия решения. Незнание правил функционирования программного обеспечения, как нам представляется, не даст судье проверяющей инстанции никакой возможности оспорить

судебное решение, основываясь на существующих правилах пересмотра.

Данная выборка проблем устранимого характера, разумеется, не является исчерпывающей. К таким проблемам также можно отнести увеличение процента цифровой безграмотности населения, включая юристов; снижение доверия к суду; риск приватизации правосудия со стороны legaltechs, которые разрабатывают предиктивное правосудие, укрепление цифрового неравенства граждан, дистанцирование участников судопроизводства, проблемы структурирования судебных решений, проблемы уравнивающей и распределяющей справедливости, стагнация и смерть континентального права и проч.

Заключение. Стоит ли, при этом, говорить о целесообразности внедрения предиктивного правосудия в систему континентального права?

Представляется, что отвергать полностью эту идею будет нецелесообразно, однако ее необходимо несколько видоизменить под существующую специфику. В виде ответов на вопросы это будет представляться лучше всего.

1. Ждать ли появления сильного искусственного интеллекта?

Представляется, что в этом нет необходимости. Во-первых, научные дискуссии касательно не только его трансформирующей роли, но и апокалиптического характера не утихают до сих пор, что, возможно, привело к существующим на сегодняшний день мораториям на разработку сильного искусственного интеллекта.

Более того, с открытием сильного искусственного интеллекта потребность в алгоритмах предиктивного правосудия отпадет за ненадобностью. Если на сегодняшний день данная технология носит несовершенный характер, это не значит, что завтра состояние будет прежним.

Кроме того, нам представляется, что данная технология нуждается в разработке именно внутри каждого конкретного правопорядка, который и сможет её настроить в связи с особенностями своего собственного процессуального права.

2. Сохранять прежнюю модель функционирования предиктивного правосудия?

Если взять в пример Россию, то здесь переопределение идеи предиктивного правосудия может выглядеть следующим образом:

В первую очередь, предлагаемая модель должна основываться на коллаборации специалистов в области права и информационных технологий соответственно их профессии. Юристы осуществляют «переработку» правовых норм, рассчитанных на включение в алгоритм, а также в рамках машиночитаемой логики устанавливают приоритет одних правил над другими; технические специалисты, в свою очередь, разрабатывают алгоритм, который будет действовать подобно

«пирамиде норм», что позволить автоматизировать не обработку большого и открытого массива данных вкупе с обработкой естественного языка, а продвинется в пользу юридического мышления, применяющего те или иные статьи сообразно фактическим обстоятельствам дела.

3. Каким образом достичь этого?

Высшие судебные органы (Верховный суд) должны переработать эти нормы, чтобы в форме, подобной обобщению судебной практики (которые служат руководящими положениями для нижестоящих судов в РФ), сформировать необходимую для обработки выборку.

Нам представляется, что псевдоалгоритмической обработке должны поддаваться не все нормы, регулирующие рассмотрение всех споров. Большего эффекта можно достичь, применяя секторальную выборку.

Для того чтобы их выделить, судам необходимо провести статистический анализ споров в зависимости от их сложности, частоте обжалования решений суда, а также фактической реализации «состязательной напряжённости» по смыслу активного противоборства сторон в ходе рассмотрения дела по существу. Кроме того, учёту должны подлежать те споры, нормативное регулирование которых в наименьшей мере поддавалось изменениям, равно как и подходы к разрешению этих дел со стороны судейского корпуса.

В отечественной научной мысли уже существуют подобные предложения: автоматизировать дела, рассматриваемые в порядке приказного, особого, упрощенного производства, расширение категорий дел об административных правонарушениях, а также некоторые корпоративные споры [14; 164]. Данные предложения должны быть учтены, но необходимо продолжать работу по выявлению категорий дел, которые могут быть автоматизированы.

Выборка на этой основе позволит создать «пул» тех споров, которые потенциально должны войти в алгоритмическую обработку.

Разумеется, такая техника должна служить исключительно в качестве инструмента поддержки по принятию решений, который будет активно администрироваться и оперативно калиброваться ввиду изменений в законодательстве и/или судебной практики.

Список использованных источников:

1. Livre blanche. Intelligence artificielle. Une approche européenne sur l’excellence et la confiance: [Adopté par Comission européennce]. – 2020. – 31 p.

2. Larret-Chahine L. L’éthique de la justice prédictive / L. Larret-Chanine // Enjeux numériques.– 2018. – N°3, p. 91.

3. G'sell F. Justice Numérique / F. G’sell // Dalloz. – 2021. – 192 p.

4. Арбузов Д. А. Перспектива применения искусственного интеллекта в гражданском процессе Российской Федерации / Д. А. Арбузов // Юридические науки: актуальные вопросы теории и практики : сб. статей V Междунар. науч.-практ. конф. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.). – 2022. – С. 192-195.

5. Guével D. Intelligence artificielle et décisions juridictionnelles. Éditions de la Maison des sciences de l'homme / D. Guével // Quaderni. – 2019/1. – n° 98. – PP. 51-59.
6. Немецкие цивилисты о юриспруденции: Юлиус фон Кирхманн, Карл Ларенц / Ю. Кирхманн — «Издательские решения», 2022. – 37 с.
7. Confions la justice à l'intelligence artificielle! [Электронный ресурс] - Режим доступа: https://www.lesechos.fr/2016/09/confions-la-justice-a-lintelligence-artificielle-1112668 (дата обращения: 15.05.2023).
8. Кравчук Н.В. Искусственный интеллект как судья: перспективы и опасения / Н.В. Кравчук // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. – 2021. – №1. – С. 115-122.
9. Kirat T., Tambou O., Do V., Tsoukias A. Equité et explicabilité des algorithmes d'apprentissage automatique: un défi technique et juridique / T. Kirat, O. Tambou, V. Do, A. Tsoukias // HAL Archives. – 2022. – 48 p.
10. Шушеначев А.В., Назаров А.Д. Этический аспект применения цифровых технологий в правоохранительной сфере / А.В. Шушеначев, А.Д. Назаров // «Вопросы российского и международного права». Том 11. – 2021. – № 11А. – С. 80-87.
11. Wouters M. La prédiction algorithmique, augure d'une meilleure justice ? Réflexions autour de la justice prédictive / M. Wouters // Faculté de droit et de criminologie, Université catholique de Louvain. – 2021. – 72 p.
12. Hubert M. Les algorithmes prédictifs au service du juge: vers une déshumanisation de la justice pénale? Regards critiques de juges d'instruction / M. Hubert // Faculté de droit et de criminologie, Université catholique de Louvain. – 2020. – 131 p.
13. Biard A. Justice en ligne ou nouveau far WWW.EST? La difficile régulation des plateformes extrajudiciaire des litiges. De Boeck Supérieur / A. Biard // Revue internationale de droit économique. – 2019. – №2, t. XXXIII. – PP. 165-191.
14. Анисимова А. С. К вопросу о возможностях использования технологий искусственного интеллекта в правосудии / А.С. Анисимова, М.П. Спиридонова // Юридический вестник ДГУ. – 2021, Т. 39. – № 3. – С. 161-165.

УДК 343.98:004.8

Кубасов Игорь Анатольевич
Профессор кафедры информационных технологий
Академии управления МВД России,
доктор технических наук, доцент,
г. Москва, Российская Федерация

ОБЕСПЕЧЕНИЕ ДОВЕРИЯ К ИСКУССТВЕННОМУ ИНТЕЛЛЕКТУ В СУДЕБНОЙ И ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Актуальность темы статьи обусловлена тем, что роль и значимость искусственного интеллекта в цифровой трансформации всех сфер жизнедеятельности, в том числе в судебной и правоохранительной деятельности, сложно переоценить. При этом обеспечение доверия к искусственному интеллекту имеет решающее значение в успешной реализации цифровой трансформации. В статье исследованы преимущества применения доверенного искусственного интеллекта и проблемные вопросы обеспечения доверия к искусственному интеллекту в судебной и правоохранительной деятельности. Обоснованы рекомендации по обеспечению доверия к системам искусственного интеллекта, а также порядок разработки и применения доверенного искусственного интеллекта в судебной и правоохранительной деятельности. Выявлена необходимость разработки стандартов контроля уровня доверия и защищенного исполнения искусственного интеллекта в судебной и правоохранительной деятельности.

Ключевые слова: искусственный интеллект; системы искусственного интеллекта; доверенный искусственный интеллект; судебная и правоохранительная деятельность.

Аннотация. Мақала тақырыбының өзектілігі жасанды интеллекттің өмірдің барлық салаларын, соның ішінде сот және құқық қорғау қызметін цифрлық трансформациялаудағы рөлі мен маңыздылығын асыра бағалау қиын екендігіне байланысты. Бұл ретте жасанды интеллектке деген сенімді қамтамасыз ету цифрлық трансформацияны табысты іске асыруда шешуші мәнге ие. Мақалада сенімді жасанды интеллектті қолданудың артықшылықтары және сот және құқық қорғау қызметінде жасанды интеллектке деген сенімді қамтамасыз етудің проблемалық мәселелері қарастырылған. Жасанды интеллект жүйелеріне сенімділікті қамтамасыз ету бойынша ұсыныстар, сондай-ақ сот және құқық қорғау қызметінде сенімді жасанды интеллектті әзірлеу және қолдану тәртібі негізделген. Сот және құқық қорғау қызметінде жасанды интеллекттің сенім деңгейін бақылау және қорғалған орындалу стандарттарын әзірлеу қажеттілігі анықталды.

Түйінді сөздер: жасанды интеллект; жасанды интеллект жүйелері; сенімді жасанды интеллект; сот және құқық қорғау қызметі.

Annotation. The relevance of the topic of the article is due to the fact that the role and importance of artificial intelligence in the digital transformation of all spheres of life, including in judicial and law enforcement activities, is difficult to overestimate. At the same time, ensuring trust in artificial intelligence is crucial in the successful implementation of digital transformation. The article examines the advantages of using trusted artificial intelligence and problematic issues of ensuring trust in artificial intelligence in judicial and law enforcement activities. The recommendations on ensuring trust in artificial intelligence

systems, as well as the procedure for the development and application of trusted artificial intelligence in judicial and law enforcement activities are substantiated. The necessity of developing standards for monitoring the level of trust and protected execution of artificial intelligence in judicial and law enforcement activities has been identified.
Keywords: artificial intelligence; artificial intelligence systems; trusted artificial intelligence; judicial and law enforcement activities.

Введение. В современных условиях искусственный интеллект выступает драйвером развития цифровой трансформации различных сфер жизнедеятельности общества. Не являются исключением судебная и правоохранительная деятельность. Однако, современное применение систем и технологий ИИ сталкивается с рядом проблем, требующих безотлагательного решения [1].

Одной из основных комплексных проблем является обеспечение доверия к системам искусственного интеллекта, применяемым в судебной и правоохранительной деятельности.

Понятие доверенного искусственного интеллекта зафиксировано в «Руководстве по этике для надежного ИИ» Группы экспертов высокого уровня по искусственному интеллекту Еврокомиссии (Ethics guidelines for trustworthy AI, 2019) [2]. Согласно этому документу, доверенный ИИ должен обладать следующими базовыми характеристиками:

законный - соответствующий применимому законодательству;

этичный - соответствующий принятым этическим принципам и ценностям;

робастный - надежный с технической точки зрения и разработанный с учетом актуального социального контекста.

В России понятие доверенного ИИ с марта 2021 года отражено в стандарте ГОСТ Р 59 276−2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения»[23] [3].

Доверие к системам искусственного интеллекта является важнейшим условием, определяющим возможность применения этих систем для решения ответственных задач обработки данных [4]. Примерами таких задач являются поддержка принятия судебных решений, беспилотное управление транспортными средствами и многие другие, ошибки при решении которых могут привести к тяжким последствиям, связанных с угрозой жизни и здоровью людей, серьезному экономическому и экологическому ущербу [5].

В рамках данной статьи исследованы проблемные вопросы обеспечения доверия к искусственному интеллекту и обоснованы рекомендации по обеспечению доверия, а также порядок разработки и применения доверенного искусственного интеллекта в судебной и правоохранительной деятельности.

[23] Доверие к системе искусственного интеллекта - уверенность потребителя, и при необходимости, организаций, ответственных за регулирование вопросов создания и применения систем искусственного интеллекта, и иных заинтересованных сторон в том, что система способна выполнять возложенные на нее задачи с требуемым качеством.

Преимущества применения доверенного искусственного интеллекта в судебной и правоохранительной деятельности

В последние годы ИИ становится неотъемлемой частью судебной и правоохранительной деятельности, и ожидается, что в ближайшие годы он произведет технологическую революцию в этой деятельности.

Можно с уверенностью предполагать о перспективах широкого применения доверенного ИИ в судебной и правоохранительной деятельности. Например, алгоритмы ИИ можно использовать для быстрого и точного анализа больших объемов данных, что может помочь сотрудникам принимать более обоснованные решения, выявлять закономерности и аномалии, а также анализировать сложные случаи. Инструменты прогнозирования для полиции на базе ИИ могут анализировать данные о преступлениях, чтобы выявлять закономерности и прогнозировать, где могут произойти преступления. ИИ также можно использовать для автоматизации рутинных задач, высвобождая время сотрудников для того, чтобы они могли сосредоточиться на решении других важных задач. Это может помочь более эффективно использовать ресурсы и снизить общий уровень преступности.

ИИ также можно использовать для выявления подозреваемых и сбора улик. Например, технологию распознавания лиц можно использовать для идентификации подозреваемых на фотографиях и видео. Криминалистические инструменты на базе ИИ также можно использовать для анализа ДНК и других типов доказательств. Эти инструменты могут помочь правоохранительным органам быстрее и точнее раскрывать преступления на основе установления криминалистически важных признаков [6, 7].

Более того, ИИ может помочь повысить эффективность и точность судебных процессов. Например, алгоритмы ИИ можно использовать для анализа юридических документов и быстрого и точного определения соответствующей информации. Это может помочь сократить время и затраты, связанные с судебными разбирательствами, а также повысить объективность юридических решений.

Одним из наиболее значительных преимуществ доверенного ИИ в судебной деятельности является то, что он может помочь в анализе и управлении огромными объемами юридических данных. ИИ можно использовать для обзора и анализа прецедентного права и судебных прецедентов, что может помочь юристам и судьям принимать более обоснованные решения. Инструменты для юридических исследований на базе ИИ также могут помочь сэкономить время и деньги, автоматизировав процесс юридических исследований и проверки документов.

ИИ также можно использовать в зале суда, чтобы помочь судьям и адвокатам подготовиться к судебным процессам. Например, чат-боты на базе ИИ могут помогать сторонам в судебном процессе, отвечая на их вопросы и предоставляя соответствующую юридическую информацию. ИИ также может помочь юристам и судьям подготовиться к судебным процессам, предсказывая исход дел на основе прошлых решений и судебных прецедентов.

Следует отметить, что важно, чтобы потенциальные преимущества ИИ сопоставлялись с проблемами обеспечения доверия к ИИ, и чтобы были предприняты шаги для обеспечения ответственного и этичного применения ИИ в судебной и правоохранительной деятельности.

Проблемные вопросы обеспечения доверия к искусственному интеллекту

Одной из основных проблем, связанных с обеспечением доверия, является потенциальная систематическая ошибка в алгоритмах ИИ. Системы ИИ обучаются на основе вводимых в них данных. Если данные, используемые при обучении, содержат систематическую ошибку, модель ИИ также будет иметь систематическую ошибку, что приведет к дискриминационным результатам. Например, если обучающие данные, используемые для создания модели ИИ в судебной системе, содержат расовую предвзятость, решения о вынесении приговора, принимаемые системой, также будут предвзятыми. Это может привести к несправедливому отношению к определенным группам в обществе. Если система ИИ используется для прогнозирования преступлений, а используемые исторические данные содержат ошибки, система будет давать неточные прогнозы, что приведет к неправомерным арестам и неправомерным осуждениям.

Еще одной проблемой использования ИИ в судебной и правоохранительной деятельности является вопрос прозрачности. Процесс принятия решений в системах ИИ часто непрозрачен, без четкого объяснения того, как система пришла к тому или иному решению. Это отсутствие прозрачности может привести к недоверию и сомнениям в надежности систем ИИ в судебном и правоохранительном секторах. Общественность потребует знать, как были приняты решения и как работает система, что может стать проблемой для разработчиков и пользователей систем ИИ. Алгоритмы ИИ часто рассматриваются как «черные ящики», а это означает, что может быть трудно понять, как алгоритм пришел к конкретному решению.

Использование ИИ в этих сферах деятельности также может привести к этическим проблемам, таким как нарушение конфиденциальности. Данные обучения, используемые для создания моделей ИИ, часто содержат личную информацию. Системы искусственного интеллекта также могут собирать личные данные отдельных лиц без их согласия. Существует также риск того, что

использование ИИ может привести к нарушению прав на неприкосновенность частной жизни, поскольку алгоритмы ИИ могут собирать и анализировать огромные объемы конфиденциальных данных. Это может нанести ущерб репутации судебной и правоохранительной системам.

Кроме того, применение ИИ в судебной и правоохранительной деятельности может привести к сокращению рабочих мест. Хотя ИИ может помочь юристам и судьям в их работе, он не может заменить человеческие суждения и навыки принятия решений, которые имеют решающее значение для правовой системы. По мере того как системы ИИ становятся все более распространенными, они могут заменить часть сотрудников, что приведет к потере рабочих мест. Это может оказать значительное влияние на рабочую силу в этих секторах и может привести к социальным и экономическим проблемам.

Правовая система должна тщательно рассмотреть преимущества и риски ИИ и найти правильный баланс между использованием ИИ и ролью человеческого суждения [8].

При этом весьма актуальной является необходимость разработки стандартов контроля уровня доверия и защищенного исполнения ИИ в судебной и правоохранительной деятельности [9, 10].

Рекомендации по обеспечению доверия к системам искусственного интеллекта в судебной и правоохранительной деятельности

Чтобы обеспечить доверие к ИИ, предлагается воспользоваться несколькими рекомендациями при разработке и эксплуатации систем ИИ в судебной и правоохранительной деятельности.

Во-первых, системы ИИ должны строиться на этических принципах и стандартах, в которых приоритет отдается справедливости, прозрачности и подотчетности. Это означает, что ИИ должен быть разработан таким образом, чтобы избежать предвзятости в данных и алгоритмах, а права человека и этические соображения должны учитываться на каждом этапе разработки и развертывания. Крайне важно привлекать различные заинтересованные стороны к проектированию, разработке и внедрению систем ИИ, включая юристов, социологов, специалистов по этике, представителей гражданского общества.

Во-вторых, системы ИИ должны подвергаться тщательному тестированию и проверке, чтобы гарантировать их точность и надежность. Модели ИИ должны быть проверены на соответствие соответствующим эталонным показателям и проверены на их чувствительность к различным входным данным, сценариям и контекстам. Более того, системы ИИ должны быть проверяемыми и объяснимыми, позволяя пользователям понимать, как принимаются решения, и оспаривать их в случае ошибок или предубеждений.

В-третьих, необходимо постоянно контролировать и оценивать системы ИИ для оценки их влияния на правосудие и общественную безопасность. Это включает в себя отслеживание производительности систем ИИ в реальных условиях, сбор отзывов от пользователей и заинтересованных сторон, а также анализ последствий решений ИИ для отдельных лиц и сообществ. Регулярный аудит может помочь гарантировать, что системы ИИ останутся справедливыми, прозрачными и подотчетными с течением времени.

В-четвертых, системы ИИ должны развертываться таким образом, чтобы уважать права человека и укреплять доверие к системе правосудия. Это означает, что ИИ следует использовать не для замены человеческого суждения или усмотрения, а для их усиления. Более того, ИИ следует использовать таким образом, чтобы уважать конфиденциальность, защиту данных и права на надлежащую правовую процедуру.

Наконец, системы ИИ должны подлежать независимому надзору и регулированию, чтобы обеспечить их соответствие этическим стандартам и требованиям законодательства. Это можно сделать с помощью сочетания механизмов внутреннего и внешнего аудита, включая советы по этике, независимых аудиторов и регулирующие органы.

Таким образом, ИИ может помочь укрепить правосудие и обеспечить общественную безопасность, сохраняя при этом доверие общественности к правоохранительной системе.

Порядок разработки и применения доверенного искусственного интеллекта в судебной и правоохранительной деятельности

Применение ИИ в судебной и правоохранительной деятельности требует ответственного рассмотрения и системного подхода в обеспечении общественной безопасности и защиты прав человека. Предлагаем следующий порядок разработки и применения доверенного искусственного интеллекта.

Шаг 1. Определение цели интеграции ИИ.

Первым шагом в интеграции ИИ в судебную и правоохранительную деятельность является определение цели его применения. ИИ можно использовать для различных целей, включая ведение дел, анализ доказательств и принятие решений. Предполагаемая цель интеграции ИИ должна быть четко определена, чтобы гарантировать, что его применение оправдано, а любые риски, связанные с его применением, идентифицированы и устранены.

Шаг 2: Задание (установление) этических принципов.

Интеграция ИИ должна осуществляться в соответствии с этическими принципами, которые обеспечивают его ответственное, прозрачное и подотчетное использование. Эти руководящие принципы должны быть заданы с участием заинтересованных сторон, включая

юристов, специалистов по данным и представителей гражданского общества. Руководящие принципы должны охватывать такие вопросы, как конфиденциальность данных, непредвзятость и объяснимость.

Шаг 3: Выбор и предварительная обработка релевантных данных.

Точность ИИ зависит от качества и количества данных, используемых для его обучения. Поэтому важно выбрать соответствующие данные, которые являются релевантными и объективными. Данные также должны быть собраны этично и законно, люди должны быть проинформированы и дать свое согласие на использование их данных. Перед обучением модели ИИ данные должны быть предварительно обработаны, чтобы убедиться, что они чистые, актуальные и беспристрастные. Методы предварительной обработки данных следует использовать для устранения любых систематических ошибок, которые могут существовать в данных.

Шаг 4: Обучение модели ИИ.

Модели ИИ должны быть обучены на выбранных данных, чтобы они могли делать точные и надежные прогнозы. Процесс обучения должен быть прозрачным, а любые отклонения в данных должны быть устранены, чтобы гарантировать, что модель ИИ является справедливой и беспристрастной.

Шаг 5. Внедрение ИИ в судебную и правоохранительную деятельность.

После обучения модели ИИ ее можно применять в судебной и правоохранительной деятельности. Тем не менее, его использование должно тщательно контролироваться, чтобы гарантировать, что он работает по назначению и не причиняет вреда людям. Любые ошибки или предубеждения должны быть выявлены и незамедлительно устранены.

Шаг 6: Оценка производительности ИИ.

Производительность ИИ необходимо регулярно оценивать, чтобы убедиться, что он соответствует своей цели и не причиняет вреда. Эта оценка должна проводиться независимыми экспертами, обладающими необходимым опытом для оценки эффективности моделей ИИ.

Шаг 7: Постоянно улучшение модели ИИ.

Модели ИИ необходимо постоянно улучшать, чтобы они оставались точными и надежными. Этот процесс улучшения должен руководствоваться этическими принципами, разработанными на шаге 2, и любые улучшения должны быть прозрачными и подотчетными.

Заключение. Обеспечение доверия к ИИ в судебной и правоохранительной деятельности имеет решающее значение. С учетом вышеизложенных рекомендаций по обеспечению доверия, а также предложенного порядка разработки и применения доверенного искусственного интеллекта, разработчикам следует создавать системы ИИ, которым можно доверять в техническом и психологическом плане.

Список использованных источников:

1. Кубасов И.А. Проблемные вопросы применения технологий искусственного интеллекта в деятельности органов внутренних дел Российской Федерации. Вестник Воронежского института МВД России. 2021. № 3. С. 180-186.

2. Права человека в эпоху искусственного интеллекта: Европа как созидатель международных стандартов в области искусственного интеллекта // Бюллетень Европейского Суда по правам человека. 2021. № 2(224). С. 142-144.

3. ГОСТ Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения».

4. Намиот Д.Е., Ильюшин Е.А., Пилипенко О.Г. Доверенные платформы искусственного интеллекта. International Journal of Open Information Technologies. 2022. Т. 10. № 7. С. 119-127.

5. Кубасов И.А., Сушков В.И. Применение технологий искусственного интеллекта в робототехнических комплексах специального назначения в целях обеспечения правоохранительной деятельности. Вестник Воронежского института ФСИН России. 2022. № 3. С. 69-76.

6. Кубасов И.А. Разработка методов ДНК-фенотипирования для расследования и раскрытия преступлений. Вестник Воронежского института МВД России. 2022. № 2. С. 166-172.

7. Кубасов И.А. Информационные технологии в следственной и судебно-экспертной деятельности. В сборнике: Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации. Сборник научных статей по материалам международной научно-практической конференции. Под редакцией Ю.В. Гаврилина, Ю.В. Шпагиной. Москва, 2021. С. 171-177.

8. Ивлиев Г.П., Егорова М.А. Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта. Журнал российского права. 2022. Т. 26, № 6. С. 32-46.

9. Кубасов И.А., Шапкин А.В. Разработка стандартов контроля уровня доверия к нейросетевым приложениям искусственного интеллекта, применяемых подразделениями МВД России. В сборнике: Стратегическое развитие системы МВД России: состояние, тенденции, перспективы. Сборник статей Международной научно-практической конференции. Под общей редакцией И. Г. Чистобородова, А. Л. Ситковского, В. О. Лапина. 2020. С. 428-435.

10. Шапкин А. В., Кубасов И. А., Иванов А. И. Развитие отечественного нейросетевого искусственного интеллекта в защищенном исполнении. Вестник Воронежского института ФСИН России. 2019. № 4. С. 132-144.

ӘОК 343

Маханов Талғат Ғабитұлы
Қазақстан Республикасы Бас прокуратурасының жанындағы
Құқық қорғау органдары академиясының Ведомствоаралық ғылыми-
зерттеу институтының аға ғылыми қызметкері, құқықтану магистрі,
Қазақстан Республикасы, Астана қ.

Мұқатаев Талғат Маратұлы
Қазақстан Республикасы Бас прокуратурасының жанындағы
Құқық қорғау органдары академиясының Ведомствоаралық ғылыми-
зерттеу институтының аға ғылыми қызметкері
Қазақстан Республикасы, Астана қ.

КРИПТОВАЛЮТАНЫ ҚОЛДАНУ АРҚЫЛЫ ЖАСАЛАТЫН ҚЫЛМЫСТАРҒА ҚАРСЫ ІС-ҚИМЫЛДАҒЫ ЖАСАНДЫ ИНТЕЛЛЕКТТІҢ РӨЛІ

Аннотация. Мақала криптовалютаны қолданумен байланысты қылмыстарға қарсы іс-қимылда жасанды интеллекттің рөлі тақырыбына арналады. Мақалада Қазақстан Республикасы цифрлық активтерді реттеу жөнінде қабылданып отырған шаралар қарастырылып, жасанды интелекттің мәні ашылады. Сонымен қатар, криптовалютаны реттеу бойынша жасанды интеллектті қолдану жөніндегі ғалымдардың пікірі талданады. Зерттеу нәтижелері бойынша, авторлар жасанды интеллектті аталған қылмыстарға қарсы іс-қимыл бойынша мемлекеттік органдардың қызметінде қолдануға болады деген қорытынды болжам жасап, тиісті бағыттарын ұсынады.

Түйінді сөздер: криптовалюта; цифрлық активтер; жасанды интеллект; қылмыс; қарсы іс-қимыл; қаржы қызметтері; құқық қорғау органдары.

Аннотация. Статья посвящена роли искусственного интеллекта в противодействии преступности, с использованием криптовалюты. В статье рассматриваются принимаемые Республикой Казахстан меры по регулированию цифровых активов, раскрывается сущность искусственного интеллекта. Кроме того, анализируются мнения ученых по использованию искусственного интеллекта в регулировании операций с криптовалютой. По результатам исследования авторы делают прогноз-вывод о том, что искусственный интеллект возможно применим в деятельности государственных органов по противодействию указанным преступлениям, а также предлагают соответствующие пути решения.

Ключевые слова: криптовалюта; цифровые активы; искусственный интеллект; преступление; противодействия; финансовые службы; правоохранительные органы.

Annotation. The article is devoted to the role of artificial intelligence in countering crime using cryptocurrencies. The article discusses the measures taken by the Republic of Kazakhstan to regulate digital assets, reveals the essence of artificial intelligence. In addition, the opinions of scientists on the use of artificial intelligence in regulating cryptocurrency transactions are analyzed. According to the results of the study, the authors make a forecast-a conclusion that artificial intelligence may be applicable in the

activities of state bodies to counter these crimes, and also suggests appropriate ways of direction.

Keywords: cryptocurrency, digital assets, artificial intelligence, crime, counteraction, financial services, law enforcement agencies.

Қазіргі таңдағы сандық экономика аясында түрлі цифрлық активтер («криптовалюталар», түрлері шамамен 13 мыңнан аса) пайда болып, олардың виртуалды айналымы тез өсіп келеді. Кез-келген криптовалютаның негізін блокчейн технологиясы құрайды, тиісінше мәліметтер базасы түрінде ақпаратты тарату мен сақтаудың орталықтандырылмаған жүйесі болып табылады.

Блокчейннің басты артықшылығы – жиналған мәліметтердің қауіпсіздігінің жоғары деңгейі, сонымен қатар мәліметтерге жедел өзгерістер енгізу мүмкіндігі және пайдаланушыларға ұсынылатын деректердің дәлдігіне бір мезгілде кепілдік беру болып табылады. Криптовалюта платформаларының жұмысын қамтамасыз ету үшін жаңа құрылымдарды құру қызметі (әдетте блокчейндегі жаңа блоктар) майнинг болып табылады.

Цифрлық активтерді (криптовалютаны) қолдану бойынша еліміз қабылдап отырған шаралар аз емес. Мәселен, 2023 жылғы 6 ақпанда Қазақстандағы цифрлық активтер туралы заң қабылданып, 1 сәуірден бастап заңды күшіне енді.

Аталған Заң Қазақстан Республикасында цифрлық активтерді шығару және олардың айналымын және цифрлық майнинг жөніндегі қызметті реттейді[24], уәкілетті мемлекеттік орган – Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі.

Статистикалық мәліметтерге сүйенсек[25], 2023 жылғы 12 мамырдағы жағдай бойынша 258 ұйым – цифрлық майнинг саласындағы қызметтің басталғаны туралы және 57 ұйым – цифрлық майнинг өндірісіне арналған инфрақұрылымды ұсыну туралы ресми түрде хабардар етті.

Ал цифрлық активтер ұғымы және олардың түрлерін, сондай-ақ цифрлық активтерді шығару (цифрлық майнингті қоспағанда), орналастыру, айналысқа жіберу, сақтау тәртібі мен шарттарын «Астана» халықаралық қаржы орталығы[26] тиісті ережелер арқылы реттейді.

Алайда, бұл сала құқықтық реттелгенімен, криптовалютамен байланысты құқық қайшы әрекеттердің алдын алу, жолын кесу, болдырмау қаржы қызметтері мен экономикалық тергеп-тексеру органдарының басты сын-қатерлерінің біріне айналып отыр.

[24] Қазақстан Республикасындағы цифрлық активтер туралы. Қазақстан Республикасының Заңы 2023 жылғы 6 ақпандағы № 193-VII ҚРЗ // URL: https://adilet.zan.kz/kaz/docs/Z2300000193

[25] Цифрлық активтер индустриясы // URL: https://www.gov.kz/memleket/entities/mdai/activities/17673?lang=kk

[26] «Астана» халықаралық қаржы орталығы туралы. Қазақстан Республикасының Конституциялық Заңы 2015 жылғы 7 желтоқсандағы № 438-V ҚРЗ // URL: https://adilet.zan.kz/kaz/docs/Z1500000438

Мәселен, 2023 жылғы наурызда крипто айырбастау пункті арқылы цифрлық активтерді заңсыз айырбастау фактісі бойынша Қазақстанның үш азаматының заңсыз кәсіпкерлік қызметі әшкереленді. Нәтижесінде 342 мың доллар және 7 миллион теңге сомасында ақша қаражаты тәркіленді. Binance платформасында 23 мың долларға жуық криптоактивтері бар екі криптоәмиянға уақытша шектеу қойылды. Криптоәмияндарының жалпы айналымы шамамен 34 миллион долларды құраған. Тергеп-тексеру жүргізілуде[27].

Бұған дейін, бір ай бұрын Қостанай қаласында ұқсас факті бойынша шетел азаматтарына қатысты сот күдіктінің жылжымайтын мүлкіне сомасы 85 млн. теңге, яғни шамамен 187 700 доллар немесе 14 млн. рубльден астам сомаға, оның ішінде Binance криптобиржасындағы цифрлық активтерді қоса алғанда тыйым салды. Қылмыскерлер 2020 жылғы шілдеден 2023 жылғы қаңтар аралығында 180 млн. теңгеден астам заңсыз табыс тапқан (шамамен 397 500 доллар немесе 29,75 млн. рубль)[28].

Бұл санаттағы қылмыстық көріністердің әшкереленіп жатқаны санаулы деп айтса да болады, ал оның жасырынды сипатындағылар қаншама.

Осы орайда келешекте жасанды интеллект аталған қылмысқа қарсы іс-қимыл жүйесін сапалы жаңа деңгейге шығаруға қабілетті деп санаймыз. Алайда, жасанды интеллектке негізделген жаңа қосымшалардың кең әлеуеті мен біртіндеп өсіп келе жатқан саны, жасанды интеллект шешімдерінің тиімділігі мен аналитиктерді роботтармен алмастыру үшін қажетті сенім дәрежесі туралы да пікірталастар бар.

Расында да, соңғы жылдары жасанды интеллектті дамыту мәселелері жаһандану мен әлемдік экономиканы цифрландырудың негізгі факторы болып отырғаны белгілі.

Бүгінде жасанды интеллект (ағылш. Artificial intelligence, қысқ. – AI) ең алдымен бағдарламалық жүйелер мен алгоритмдер болып саналады, және де олардың басты ерекшелігін ғалымдар – адамның орнына белгілі бір есептерді шешу қабілеті деп түсінеді [1, 72 б].

Кейбір ғалымдар «ойлау және әрекет ету» парадигмасы деп аталатын жасанды интеллекттің басқа технологиялардан айырмашылығын – сыртқы әлемді сезіну, өңдеу және әсер ету қабілеттерімен жабдықталған жоғары технологиялық жүйенің объективі арқылы қарастыратынын айтады [2, 76 б].

[27] Оборот в 34 миллиона долларов: незаконный обмен криптовалюты выявили в Астане // URL: https://tengrinews.kz/kazakhstan_news/oborot-34-milliona-dollarov-nezakonnyiy-obmen-kriptovalyutyi-493130/

[28] В Казахстане арестовали имущество россиянина на $188 000 за незаконный обмен крипты // URL: https://www.forbes.ru/finansy/484986-v-kazahstane-arestovali-imusestvo-rossianina-na-188-000-za-nezakonnyj-obmen-kripty

Сонымен, заңгер-ғалым П.М. Мохат жасанды интеллектті – бұл толық немесе ішінара автономды өзін-өзі ұйымдастыратын компьютерлік-аппараттық виртуалды (virtual) немесе киберфизикалық (cyber-physical), оның ішінде био-кибернетикалық (bio-cybernetic), тірі емес, тиісті математикалық қамтамасыз етілген/бағдарламалық-синтезделген (эмулирленген) қабілеттері мен мүмкіндіктері бар жүйе (юнит) деп атайды [3, 30 б.].

Мәселен, ChatGPT және Midjourney сияқты жасанды интеллект құралдарын бизнес пен технологияға енгізу мүмкіндігі және оның қандай құндылық қосуы мүмкін екендігі туралы пікірталастар тудырып отыр Нәтижесінде көптеген жасанды интеллект негізіндегі криптовалюта жобалары қазір инвесторлардың назарын аударуда [1, 76 б].

Сонымен қатар, 2023 жылдың басында цифрлық валюталар мен жасанды интеллект криптоактивтер нарығында «жаңа трендті» орнатты, ал жасанды интеллект саласындағы дамуға байланысты жобалардың ішкі токендері бағаның өсуін жалғастыруда.

Мәселен, криптовалюталық магнат, Huobi криптобиржасының басшысы және Tron (TRX) монетасын әзірлеуші Джастин Сан[29], өз Twitterінде ChatGPT үшін жасанды интеллектке бағытталған орталықтандырылмаған төлем жүйесін құру тетігі пікірін жариялап, мұндай орта «қауіпсіз, сенімді, бұзудан, цензурадан қорғалған және жасанды интеллектті қолдауға қабілетті» орталықтандырылмаған төлем жүйесін құруға мүмкіндік беретінін айтты.

Сонымен бірге әзірлеушілер инвесторлар үшін жасанды интеллект бар ең жақсы 5 криптовалютаны ұсынып отыр:

- Fetch.ai (FET) - интернет заттарының (IOT) жұмысын қамтамасыз ететін ең жақсы жасанды интеллект;
- Vechain (VET) – жеткізу тізбегін басқаруға арналған жасанды интеллектке негізделген келешек шешім;
- SingularityNET (MAGIX) – жасанды интеллект шешімдері мен қызметтерінің ең жақсы нарығы;
- DeepBrain Chain (DBC) – жасанды интеллект пен боттарды монетизациялаудың келешек нарығы;
- Ocean Protocol (OCEAN) – жасанды интеллект жұмысын қамтамасыз ететін ең жақсы үлкен деректер протоколы[30].

Көптеген мамандардың пікірінше, жақын болашақта блокчейн, жасанды интеллект және интернеттегі байланыстар қазіргі ғылымдағы теориялық, қолданбалы ең тиімді және жылдам дамып келе жатқан бағыттардың бірі болып табылатын бір технологияға біріктіріледі.

[29] Новый тренд на рынке. Почему монеты из сферы ИИ стремительно дорожают // URL: https://www.rbc.ru/crypto/news/63e13a189a794766285ce269

[30] 5 лучших криптовалютных проектов с искусственным интеллектом // URL: https://www.buybitcoinbank.com/ru/криптовалюта/лучшие-криптовалютные-проекты-ai

Дегенмен, жасанды интеллекттің криптовалюталарға жалпы әсерін бағалау әлі ерте. Жасанды интеллект криптовалюталары мем сияқты серпін алуы немесе нарықтың негізгі динамикасын өзгерте алуы мүмкін.

Лондон Университеттік колледжінің және Principal Scientist Nokia Bell Labs профессоры Ник Лэйннің айтуынша, егер бұрын қабырғаға салынған сенсор біреудің өтіп кеткенін ғана түсінсе, болашақта ол кімнің нақты өткенін ғана емес, сонымен қатар адамның өзін қалай ұстайтынын белгілеп қана қоймай, не қажет екенін, ол өзіне немесе айналасындағыларға қауіп төндіре ме екенін айта алатын болады[31].

Қазірдің өзінде адам орындаған жұмыс, тапсырма мен машина орындаған тапсырманың аражігін ажырату, яғни адам немесе машина екенін түсіну қиын болып барады. Оған мысал – ChatGPT чат-боты, Midjourney жасанды графикасы және т.б.

Кешегі ғылыми-фантастикалық туындылардың бүгінгі күні іске асып отырғанына куә болып отырмыз (ұялы иелефон, компьютер, роботтандыру және т.б.). Әрине, бүгінгі болжам тұжырымның ертеңгі шындыққа ұласатынына кім кепіл?

Ресейлік ғалым С.А. Соменков, жасанды интеллект біздің өмірімізді қазіргі күннің өзінде өзгертуде. Бұл игілікке немесе проблемаға айнала ма, жоқ па? Ол – көбіне адамдарға байланысты. Қалай болғанда да, оны енгізу қазірдің өзінде белгілі бір әлеуметтік салдарды тудыратынын айтып отыр [4, 85 б.].

Оған қоса, отандық ғалымдар цифрлық активтерді дамыту және оларды экономикаға терең енгізу Қазақстанның қаржы жүйесінің архитектурасын біртіндеп және тез өзгертеді деп санайды (мұны қазіргі заманғы шындықтың берілуі деп санауға болады) [5, 106-б].

Сонымен қорыта келе, цифрлық активтерді (криптовалютаны) қолданумен байланысты қылмыстық құқық бұзушылықтарға қарсы іс-қимыл жүйесінде қауіптердің үнемі өсіп келе жатқан деңгейін және талдау үшін деректер көлемінің ұлғаюын ескере отырып, тиімділіктің төмендігі байқалғандықтан, жасанды интеллектті криптовалюта саласында да, жалпы қаржы жүйесінде де қолдану мүмкін деп пайымдаймыз.

Осыған байланысты қазіргі таңда қылмыстық криптовалюталар саласында: терең ғылыми-іргелі зерттеулер; қаржы қызметтері мен қылмыстық құдалау органдары мамандарының жоғары білікті әлеуеті (семинарлар, тренингтер өткізу, практикалық тағылымдамаларға қатысу); мемлекет тарапынан қажетті нормативтік-құқықтық әзірлемелер; халықаралық озық тәжірибелерді отандық құқық қолдану практикасына енгізу және т.б. жұмыстарды жүргізу қажет деп санаймыз.

[31] Ксения Гогитидзе, Би-би-си, Лондон. Искусственный интеллект - угроза или помощник для человечества? / URL: https://www.bbc.com/russian/features-38931070

Қолданылған әдебиеттер тізімі:

1. Соколова И.С., Гальдин А.А. Практическое применение искусственного интеллекта в условиях цифровой экономики // Модели, системы, сети в экономике, технике, природе и обществе. 2018. №2 (26). – С.71-79.

2. Vasiliev, A. A., & Pechatnova, Yu. V. (2020). The position of the artificial intelligence among the elements of the legal relationship. Digital Law Journal, 1(4), 74–83.

3. Морхат П.М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы // дисс. на соискание учёной степени доктора юридических наук, Москва 2018. – 420 с.

4. Соменков С.А. Искусственный интеллект: от объекта к субъекту? Вестник Университета имени О.Е. Кутафина (МГЮА). 2019, (2). – С.75-85.

5. Қойшыбайұлы Қ. Копбаев Д.З. Бидайшиева А.Б. Правовое регулирование блокчейн и криптовалют: проблемы и перспективы выкуска токенов и их оборот на территории Республики Казахстан // Вестник Института законодательства и правовой информации Республики Казахстан, Том 1 № 72 (2023). – С.98-107.

Момотов Виктор Викторович
Председатель Совета судей Российской Федерации, судья, секретарь Пленума Верховного Суда Российской Федерации,
г. Москва, Российская Федерация

Доклад на тему:

СУДОПРОИЗВОДСТВО В РОССИИ В УСЛОВИЯХ НОВЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

В последние десятилетия использование и применение новых цифровых технологий и систем искусственного интеллекта в той или иной степени сопровождают все сферы жизнедеятельности современного общества, в том числе и судебную систему. Уже стало очевидным то, что повышение эффективности и качества правосудия является невозможным без внедрения и использования передовых технологий и решений.

Например, в нашей стране в целях дальнейшего развития информатизации судебной системы и сервисов электронного правосудия постоянно улучшается обеспеченность судов компьютерной техникой, с 2020 года для судебной системы закупается ежегодно не менее 10 тысяч персональных компьютеров. Обеспечиваются круглосуточная доступность и функционирование более 10 тысяч официальных сайтов федеральных судов, органов судейского сообщества, органов Судебного департамента и участков мировых судей.

Наличие цифровых ресурсов позволяет гражданам и организациям с помощью сервисов электронного правосудия реализовывать в удобном для них формате процессуальные права и обязанности, закрепленные за ними законом. Возьмем хотя бы возможность направления в суд процессуальных обращений и документов в электронном виде через сайт в интернете и получения ответа на обращение либо копии вынесенного по делу судебного акта, заверенного цифровой подписью судьи, или проведения судебного заседания с применением систем видеоконференц-связи, – участникам процесса доступно совершение таких процедур из любого места, где бы они не находились, без затраты времени и средств на физическое посещение суда.

Несомненно, эти возможности оказывают влияние на правовую культуру и правосознание общества, поскольку правосудие становится ближе, прозрачнее и доступнее. Об этом свидетельствует тот факт, что электронные судебные сервисы с каждым годом становятся все более популярными и востребованными у участников судопроизводства, а также статистические сведения, согласно которым за последние шесть

лет количество обращений в судебные органы через интернет-порталы превысило 10 миллионов.

В России на 2024 год запланирован запуск суперсервиса «Правосудие онлайн» с применением цифровых технологий и технологий искусственного интеллекта.

В суперсервис, кроме ранее введенных в действие электронных инструментов, будут встроены вспомогательные элементы, с помощью которых можно определить подсудность дела, рассчитать и оплатить госпошлину, а также стандартные формы и справочники исковых требований. Кроме того, суперсервис будет интегрирован с другими государственными информационными системами, что будет способствовать созданию единого цифрового пространства и упрощению сбора и проверки необходимых сведений и материалов.

Таким образом, можно с уверенностью констатировать, что судебная власть в России не отстает от текущих в мире тенденций в плане технологической модернизации и прогресса.

Как известно, искусственный интеллект – это технология, позволяющая компьютерам осуществлять деятельность и выполнять задачи, которые подвластны интеллекту человека, его когнитивным мыслительным функциям.

Говоря об искусственном интеллекте, следует обратить внимание на различие так называемого слабого искусственного интеллекта, используемого для решения определенных узкоспециализированных задач по заранее заданному алгоритму, и сильного искусственного интеллекта, способного самообучаться и самостоятельно принимать решения, имитируя человеческий мыслительный процесс.

Применение в деятельности суда технологии слабого искусственного интеллекта позволяет уменьшить рутинную работу судей и работников аппарата суда. Уже сейчас с ее помощью можно решать задачи по автоматизированной обработке информации при осуществлении делопроизводства, рассмотрению поступающих в суд процессуальных документов в целях выявления их несоответствия требованиям процессуального законодательства, идентификации личности и полномочий для участия в судебном разбирательстве.

Потенциал использования слабого искусственного интеллекта мы рассматриваем, прежде всего, в оптимизации судебного процесса, в частности, для расшифровки аудиопротоколов судебных заседаний или составления проектов судебных актов на основе анализа текста процессуального обращения и материалов судебного дела, например, в приказном производстве при рассмотрении гражданских или административных дел по бесспорным требованиям, где принятие решения не связано с анализом правоотношений сторон и в большей степени имеет технический характер.

Также представляется целесообразным в перспективе изучить возможность применения подобных алгоритмов и к простым однотипным спорам с «шаблонной» фабулой, при разрешении которых также не требуется всестороннего и тщательного изучения собранных по делу доказательств.

Кроме того, на наш взгляд, имеет смысл рассмотреть доступные сегодня технологии и способности машин на предмет предотвращения указанных споров и их досудебного урегулирования. Следует помнить о том, что обращение в суд – это крайняя мера защиты своих прав. Обладая возможностью обрабатывать большие массивы информации с целью анализа и систематизации судебной практики, существующие технологические решения могли бы содействовать потенциальным истцам в получении представления о наиболее вероятном результате относительно исхода будущего спора, сроках его рассмотрения и размере судебных издержек, побуждая тем самым стороны не доводить конфликт до крайности и предотвращая инициирование споров, обреченных на неуспех.

С учетом прорыва в машинном обучении в середине 2000-х годов, сделавшего возможным обучение и применение в самых различных областях глубоких нейронных сетей, показавших свое преимущество при решении разнотипных задач: от распознавания речи и лиц до управления беспилотными транспортными средствами, повышается вероятность использования технологий искусственного интеллекта и больших данных непосредственно при осуществлении правосудия и в правоприменительной деятельности.

Вместе с тем их применение в судебной и правоохранительной системе вызывает некоторые опасения, связанные, например, с тем, что бездушные нейросети, даже со способностью к самообучению, в настоящее время не способны стать заменой когнитивным функциям человеческого мозга и увидеть все тонкости и обстоятельства конкретного дела, такие как индивидуальные особенности лица, привлекаемого к ответственности, мотивы, побудившие его к совершению правонарушения, или, например, дать оценку действиям участника гражданского оборота с точки зрения добросовестности и многое другое.

Кроме того, открытие машине необходимого ей для обучения допуска к информационным базам с персональными данными граждан повышает риск утечки конфиденциальной информации к злоумышленникам, что негативным образом способствует причинению лицу, сведения о котором были ранее закрыты, имущественного и морального вреда, связанного с неправомерным получением и распространением его личных данных.

Поэтому параллельно с введением новых технологий необходимо предпринимать шаги, которые бы нивелировали риски, связанные с их применением на практике.

Известно, что нейронные сети обладают способностью закреплять классификации или распознавать новые данные на основе ранее выявленных закономерностей, касающихся отдельных лиц, групп лиц или слоев населения, в связи с чем появляются предпосылки для дискриминации человека по различным признакам. Например, применявшаяся в США технология искусственного интеллекта при определении вероятности совершения гражданином правонарушения допускала ошибки и больше склонялась в сторону людей с черным цветом кожи, даже когда объективно такая вероятность была крайне мала.

Статистические методы обработки больших данных приводят к выявлению искусственным интеллектом определенного набора характеристик, приданию им наибольшего веса при оценке уже конкретного дела, что может повлечь нарушение принципа презумпции невиновности, когда система будет заведомо склоняться в сторону обвинения подозреваемого лица. Следовательно, в случае использования нейронных сетей в качестве помощника при принятии процессуальных решений необходимо осуществлять проверку применяемых ими алгоритмов на избыточный учет таких факторов, как пол, раса, этническое происхождение, социально-экономическое состояние, политические взгляды, социальные связи и т. д. Также не нужно забывать, что сами программы, будучи созданными людьми, содержат отражения субъективных представлений и предпочтений их авторов.

Отсутствие у искусственного интеллекта правосубъектности возлагает всю ответственность за его работу и принимаемое окончательное решение на уполномоченное лицо, в связи с чем должна быть обеспечена возможность так называемого внешнего аудита, т. е. судья и участники процесса должны иметь доступ к исходным большим данным и программным алгоритмам, используемым нейронными сетями, и понимать их логику при анализе и принятии решения для устранения неточностей в случае их выявления.

Обязательным условием использования результатов, полученных с использованием нейронных сетей, является наличие пользовательского контроля, когда право принятия окончательного решения остается за судьей.

Также существует риск того, что судьи и участники процесса начнут зависеть от заранее сделанных прогнозов относительно итогов процесса, которые базируются исключительно на объективных статистических расчетах. Судья в случае несогласия с предложенным искусственным интеллектом решением будет вынужден не только

обосновать свои выводы, но и объяснить причину такого несогласия. С учетом высокой нагрузки на судей могут возникать ситуации, когда судья предпочтет идти путем наименьшего сопротивления и соглашаться с искусственным интеллектом, а потому необходимо предусмотреть условия, которые не допустят такого автоматического засиливания решений искусственного интеллекта подписью судьи.

Подводя итог вышесказанному, необходимо отметить очевидный факт возрастания роли машины и современных технологий во всех сферах жизнедеятельности, в том числе и в судебной системе.

Однако на сегодняшний день еще довольно далеко до создания технологии настоящего сильного искусственного интеллекта, способного полностью воспроизвести человеческий разум и обладать полномочиями по осуществлению правосудия, поэтому все рассуждения на эту тему могут носить лишь гипотетический характер. На данный момент даже в долгосрочной перспективе представляется, что самообучаемые искусственные нейронные сети, предназначенные для объективной оценки доказательств и самостоятельного принятия решений, смогут принимать участие в осуществлении правосудия лишь в качестве помощника судьи, а не его полноценной замены.

Следует помнить о том, что осуществление правосудия над людьми − это живой процесс, и судья, наделенный соответствующими полномочиями, обладает необходимыми для этого качествами, такими как компетентность, справедливость, уважение к участникам процесса, порядочность и достоинство, соблюдение профессиональной тайны, наличие терпения, моральная чистоплотность, этичность и эмпатия, судья способен увидеть скрытые мотивы сторон, распознать истинные причины произошедшего события и учесть все индивидуальные особенности, которые необходимы для вынесения законного, объективного и гуманного решения.

УДК 343.11:004

Мусенова Эльвира Елеусиновна
MAQSUT NARIKBAYEV UNIVERSITY (KAZGUU)
Құқық жоғары мектебі, қылмыстық сот әділдігі департаментінің
teaching professor, заң ғылымдарының кандидаты
Қазақстан Республикасы, Астана қ.

ҚЫЛМЫСТЫҚ СОТ ІСІН ЖҮРГІЗУДЕ АҚПАРАТТЫҚ ТЕХНОЛОГИЯНЫ ҚОЛДАНУ

Аннотация. Мақалада қылмыстық сот ісін жүргізуде ақпараттық технологияларды қолдану тәртібін заңнамалық реттеудің, атап айтқанда онлайн режимде сот отырыстарын өткізуді, алқабилерді іріктеу кезінде жасанды интеллектті пайдалану мүмкіндігі, қашықтан жауап алу мәселелері қарастырылады. Цифрлық ақпарат көздерімен жұмыс жасау барысында қылмыстық процестің аясына түскен адамдардың конституциялық құқықтары мен бостандықтарын қорғау кепілдіктерін сақтау қажеттілігіне назар аударылады. Мақалада қылмыстық істер бойынша дәлелдеуде ақпараттық технологияларды пайдалануды іс жүргізуде реттеуді жетілдірудің негізгі бағыттары тұжырымдалған.

Түйінді сөздер: ақпараттық технологиялар; қылмыстық процесс; электрондық дәлелдемелер көздері; қашықтықтан жауап алу; басты сот талқылауының нысаны; кепілдіктер; жасанды интеллект.

Аннотация. В статье рассматриваются проблемные вопросы законодательной регламентации порядка применения информационных технологий в уголовном судопроизводстве, в частности проведения судебных заседаний в онлайн режиме, о возможности использования искусственного интеллекта при отборе присяжных заседателей, дистанционного допроса. Акцентируется внимание на необходимости соблюдения гарантий защиты конституционных прав и свобод граждан, вовлеченных в орбиту уголовно процесса, при работе с цифровыми источниками информации. В статье формулируются основные направления совершенствования процессуальной регламентации использования информационных технологий в доказывании по уголовным делам.

Ключевые слова: информационные технологии; уголовный процесс; электронные источники доказательств; дистанционный допрос; форма главного судебного разбирательства;, гарантии; искусственный интеллект.

Annotation. The article deals with problematic issues of legislative regulation of the procedure for the use of information technologies in criminal proceedings, in particular, conducting court sessions online, the possibility of using artificial intelligence in the selection of jurors, remote interrogation. Attention is focused on the need to comply with the guarantees of protection of the constitutional rights and freedoms of citizens involved in the orbit of the criminal process when working with digital information sources. The article formulates the main directions for improving the procedural regulation of the use of information technologies in proving criminal cases.

Keywords: information technologies; criminal proceedings; electronic sources of evidence; remote interrogation; form of the main trial; guarantees; artificial intelligence.

Мемлекет басшысы Қасым-Жомарт Тоқаевтың Қазақстан халқына Жолдауында «Түрлі өңірде ұқсас істер бойынша әртүрлі шешімдер қабылданатын жайттар жиі кездеседі. Қазір цифрлық талдау жасайтын құрал әзірленуде. Сол арқылы сот төрелігін атқару ісін біріздендіруге мүмкіндік туады. Жоғарғы Сот осы интеллектуалды жүйені толық енгізуді тездеткені жөн» деп айтылған-ды [1].

Мойындау керек, қазір ақпараттық технология дәуірі, бүгінгі таңда әлем бойынша біршама қызметтердің бөлігі автоматтандырылған және олар адамның физикалық та интеллектуалдық та жұмыстарын арнайы бағдарламалар арқылы жүзеге асырып жатқанына куә болып отырмыз. Сөзсіз техниканың тиімді жақтарын да жоққа шығармаймыз, себебі жекелелеген жұмыстардың барысын жылдамдатады, қағазбастылықтан арылтады, уақыттың тиімділігін артады, қажетті шығындарды да азайтады.

Соңғы жылдары қылмыстық сот ісін электрондық форматта жүргізу жағдайлары да көрініс алуда. ҚР ҚПК 42-1-бабына сай, қылмыстық процеске қатысушылардың пікірін және техникалық мүмкіндіктерді ескере отырып, қылмыстық сот ісін электрондық форматта жүргізуге құқылы, бұл туралы қылмыстық процесті жүргізуші адам уәжді қаулы шығарады, ал процеске қатысушының пікірі сотқа дейінгі тергеп-тексеруді жүзеге асыратын адамға, судьяға өтінішхат түрінде енгізіледі [2]. Осыған орай, сотқа дейінгі және сот сатыларында да электронды іс жүргізу өз бастамасын алған, яғни сотқа дейінгі тергеп-тексеру сатысында «е-ҚІ модулі», ал сот сатыларында «Сот кабинеті» сервисі арқылы электронды форматта біршама істер жүргізіліп жатыр.

Айта кету керек, сотқа дейінгі тергеп-тексеруді жүргізетін адам электрондық форматта іс жүргізу туралы шешімді өз бастамасымен қабылдайды, яғни электронды форматта іс жүргізудің нақты негіздерін заң айқындамай отыр, тек техниканың мүмкіндіктерін ескеру қажет деп қана көрсетеді.

«Сот кабинеті» сервисі де азаматтардың соттарға жүгіну процесін жеңілдетуге арналған, яғни сот органдарына арыз беруге, шағымдарды, өтінішхаттарды, қажетті құжаттарды, жекелеген құжаттардың көшірмелерін жолдауға, сондай-ақ судьяларға қылмыстық істерді үйлестіруге, қылмыстық істердің барысын бақылауға, соттардың қызметтеріне де баға беріп, талдау жасауға, сот тәжірибесінің жалпылаумен танысуға және т.б. жағдайларға мүмкіндігі ерекше. Ия, құжаттардың мұндай айналымдарын автоматтандыру ақылға қонымды.

«Электрондық қылмыстық іс» модулі (е-ҚІ модулі) – қылмыстық істі дайындауды, жүргізуді, жөнелтуді және сақтауды ұйымдастыруға арналған сотқа дейінгі тергеп-тексерудің бірыңғай тізілімінің функционалы. Сотқа дейінгі тергеп-тексеруді электрондық форматта жүзеге асыру, оның ішінде лауазымды адам қабылдаған процестік шешімдер мен әрекеттердің негізінде сотқа дейінгі тергеп-тексерудің

бірыңғай тізіліміне электрондық құжатты енгізу немесе PDF-құжатты салу арқылы, сондай-ақ электронды цифрлы қол қойылатын электрондық ақпараттық есеп құжаттарының қажетті деректемелерін толтыру [3]. Одан бөлек, сотқа дейінгі сатыда ҚР ҚПК 213-бабына сай, ғылыми-техникалық құралдарды пайдалана отырып, бейнебайланыс режимінде жауап алу (қашықтықтан жауап алу) мүмкіндіктері тағы бар.

Қашықтан жауап алудың нақты негіздері, тәртібі, сонымен қатар қашықтан алынған жауаптың нәтижесінде ҚР ҚПК 199-бап талаптарына сай жасалған хаттаманың дәлелдемелік күші де заңмен нақтыланып отыр. Алайда біздің пікірімізше қашықтан жауап алудың бейне жазбасын да іске хаттаманың қосымшасы ретінде, қоса тіркеу қажеттілігін заңмен реттеу орынды болар. Себебі қылмыстық процестік заңға енгізілген соңғы өзгерістердің бірі, ол ҚР ҚПК 199-бабының 3-бөлігімен байланысты болып отыр, яғни "Тергеу әрекетінің барысы мен нәтижелері дыбыс-, бейнежазба құралдарының көмегімен толық тіркелген жағдайда, тергеу әрекетін жүргізетін адам алынған нақты деректерді және іс үшін маңызы бар анықталған мән-жайларды қысқаша баяндаумен шектелуге құқылы" [4].

Ал сот отырысының барысы 347-1-бабына сай, аудио-, бейнежазба құралдарының көмегімен жүзеге асырылатындығы белгілі. Осыған орай, ҚР ҚПК 213-бабының 3-бөлігін мына мазмұнмен толықтыру орынды деген пікірдеміз: «Қашықтан жауап алу бейне-жазбасы хаттамаға қоса тіркеледі».

Одан бөлек «қашықтықтан» емес «қашықтан» деген сөз қолдану тиіс деген мамандардың пікірі де орынды. Сондықтан да ҚР ҚПК 213-бабындағы «қашықтықтан» деген сөздерді толықтай «қашықтан» деген сөздермен ауыстыру орынды болар.

Қашықтан демекші, 2020 жылдары «COVID-19» әлемдегі жағдайларға көзқарастарды түбегейлі өзгерткені тағы бар. Тіпті басты сот талқылауларын да қашықтан өткізуге мүмкіндік беретініне көз жеткіздік, олай жасамасқа да шара қалмады. Мұндай жағдайда техниканың үлесі де көмегі де орынды болды. Салдарында қашықтан өтетін сот отырыстарының оң және теріс жақтарына да баға бердік, себебі «таяқтың екі ұшының бары» белгілі.

Оған қарамастан, бүгінгі таңға дейін қылмыстық істер бойынша біршама сот отырыстарының қашықтан өтіп жатқаны тағы бар, алайа қылмыстық істер бойынша қашықтан сот отырысын жүргізуге не себеп не негіз деген сұрақтар туындайды. Оның үстіне берде-бір нормативті акт, қашықтан сот отырысын жүргізу себептері мен негіздерін реттемеген. Ия, әлем бойынша төтенше жағдайлар орын алып, ала-сапыран уақыттағы себептері мен қажеттілігін түсінуге болады. Ал бүгінгі таңда қылмыстық істер бойынша қашықтан өтіп жатқан сот отырысының себебі неде?

Мұндай сот отырыстарында негізгі қағидаттар да назардан тыс қалғандай, мәселен ҚР ҚПК 331-бабына сай, сот талқылауының тікелей

және ауызша болуы. Яғни барлық процеске қатысушылардың бір уақытта, бір жерде дәлелдемелерді толық, жан-жақты және объективті зерттеуі, тараптардың айғақтары мен дәйектері, сот отырысындағы тараптардың тікелей жарыспалылығы өте маңызды, себебі ол сот шешімінің әділдігі мен заңдылығының бірден-бір кепілі. Сол себепті мүмкіндігінше қылмыстық істер бойынша сот отырысы әдеттегідей, қалыпты жағдайда жүзеге асуы тиіс. Оның үстіне қашықтан жүргізілген сот отырысында техниканың мүмкіндігі, интернет байланысының сапасы, процеске қатысушылардың мұқияттылығы, олардың назары маңызды, ал мұндай кедергілердің орын алуы сөзсіз. Ия, қашықтан сот отырысын жүргізудің жекелеген себептері болуы мүмкін,ол себептер бойынша қашықтан сот отырысын жүргізуге болады дегенді істе білдірмейді. Біздің пікірімізше егер, қашықтан сот отырысын жүргізудің нақты дәлелді себептері орын алса, онда оны да заңмен реттеу орынды деген пікірдеміз.

Бүгінгі таңда техниканың мүмкіндігі орасан, сол себіпті де болар талқыға түсіп жатқан өзекті мәселелердің бірі, ол жасанды интеллект және оны қолдану мүмкіндігі.

Егер жасанды интеллект ұғымын дұрыс түсінсек, ол электронды заңгер, яғни робот тергеуші, не робот судья. Демек, барлық процестік әрекеттер мен шешімдерді тек техникалық бағдарламалардың орындауы болып саналады. Әрине кез-келген қызметті автоматтандыру, ол екі маманның жұмысының нәтижесі деп түсінеміз, яғни IT-маманы және заңгер (тергеуші, прокурор, судья), демек тергеуші немесе судья өздерінің білімін, біліктілігін, тәжірибесін, шығармашылығын, адамгершілігін, тіпті ар-ожданын да IT-маманының көмегі арқылы техникаға жүктейді дегенді білдіреді, нәтижесінде бұл қызметтің барысын автоматтандыру, қолдан жасалған интеллект болып шыға келетін сыңайлы.

Сонда жасанды интеллект кез келген адамның бойындағы қасиеттері мен қабілеттерін автоматтандыру деп түсінеміз бе? Демек адамның интеллектісімен санаса алатын компьютердің функциялары болғаны ма?

Алайда интеллектуалдық еңбекті автоматтандырудың өзін елестету қиын, өйткені шығармашылық процесін техникаға жүктеу қаншалықты қисынды және мүмкін деген де сұрақ туындайды.

Бүгінгі таңдағы электронды іс жүргізу форматы көріп отырғанымыздай, қылмыстық істер бойынша электрондық құжат айналымдарын, яғни лауазымды адам қабылдаған процестік шешімдер мен әрекеттерді енгізу, толтыру ол процесті жүргізуші органның тікелей басқаруымен жүргізілуде.

Ал енді, қылмыстық-процестік салада әділ және заңды шешім қабылдауды автоматтандыру мәселесі бүгінгі таңда ашық күйінде қалып отыр. Біздің пікірімізше жалпы қылмыстық істер барысын

автоматтандыру, әсіресе соттың шешімін техникаға жүктеу орынсыз, себебі мұндай процесс барысы ол компьютерлік ойын емес. Әрбір істе адамның құқықтары мен бостандықтары, тағдыры мен болашағы конституциямен қорғалатын басты құндылық. Сондықтан қылмыстық істің аясына түскен адамдардың құқықтарын, заңды мүдделері мен бостандықтарын қорғау мақсатында конституциялық және қылмыстық процесс принциптерінің де маңызы ерекше. Мәселен, Конституцияның 77-бабының 3-бөлігінде көзделгендей, сотта әркім өз сөзін тыңдатуға құқылы; айыпталушы өзінің кінәсіздігін дәлелдеуге міндетті емес; адамның кінәлі екендігі жөніндегі кез келген күдік айыпталушының пайдасына қарастырылады; заңсыз тәсілмен алынған айғақтардың заңды күші болмайды; заңды күшіне енген сот үкімімен ғана қылмысқа кінәлі деп танылады [5]. Аталған конституциялық қағидаттар әрбір адамның қорғану құқығын қамтамасыз етеді. Ал қылмыстық процесс принциптерінің маңызы да сөзссіз, себебі соттың шешімінің заңдылығы мен негізділігі, ол әрбір қылмыстық іс аясына түскен адамдардың құқықтары мен бостандықтарының қорғалуын білдіреді, оның ішінде сот ісін жүргізуді тараптардың жарыспалылығы мен тең құқылығы негізінде жүзеге асыруы (ҚР ҚПК 23-бап), сонда таразы басына салынатын тараптардың дәйектері, оның растығы немесе теріске шығаруы, ол дәлелдемелерге соттың баға беруі қалай жүзеге аспақ? Ал дәлелдемелерді ішкі сенім бойынша бағалау қағидатының мәні қайда қалмақ? Яғни судья, прокурор, тергеуші, анықтаушы дәлелдемелердің жиынтығына негізделген өзінің ішкі сенімі бойынша бағалауы, әсіресе бұл ретте заң мен ар-ожданды басшылыққа алуы (ҚР ҚПК 25-бап). Электронды жүйеде ар, ұждан деген сөздердің мәні де мағынасы да болмайтыны анық. Қылмыстық істердің жариялылығы қағидаты, яғни қылмыстық істерді талқылау барлық соттарда және сот сатыларында ашық жүргізілуі (ҚР ҚПК 29-бап) және тағы басқа принциптер [6].

Егер сот отырысы электронды түрде жүзеге асытын болса, онда қылмыстық процесс принциптерінің бірде-бірінің мәні де маңызы да болмайды, демек іс жүргізудің барлық ережелері қайта жаңаратын болғаны, ал оның салдарында моральдың, адамгершіліктің, ізгіліктің құнсыздығын білдіретін сыңайлы. Сондықтан да болашақта барлығы афтоматтандырылады дегенді елестету де оңайға соқпасы анық.

Тараптардың теңдігі мен жарыспалылығын электронды таразысы жүзеге асыратын болса, ол адамдардың құқықтары мен бостандықтарының қорғалуын қамтамасыз ете алатыны күмәнды.

Десек те, біз бұл жағдайға орынды баға бере алмағанмен, барлығы уақыттың еншісінде екенін тағы да мойындаймыз.

Жоғарыда атап өткендей, электронды іс жүргізудің кейбір тиімді жақтарын да жоққа шығармаймыз, сол себепті жасанды интеллект ретінде толықтай автоматтандыру емес, бәлкім ішінара, яғни жекелеген әрекеттерді қарастыруға болатын шығар. Мәселен сот отырысының үш

нысанда, яғни жалпы, қысқартылған және күрделенген нысанды жүргізілетіні белгілі. Осыған орай, әрбір сот отырысының өзіндік ерекшеліктері тағы бар. Әсіресе күрделенген сот отырысы, ол іске алқабилердің қатысуымен жүргізілуіне байланысты. Алқабилер қатысатын сот отырысының дайындық бөлігі, сот тергеуі, сот жарыссөзі өз алдына талаптар қояды. Оның ішінде алқабилерге кандидаттарды шақырту, олардың ішінде сот талқылауына қатысу үшін алқабиге кандидаттарды іріктеудің өзі ұзақ уақытта қажет етеді.

Оның үстіне ҚР ҚПК 638-баптың екінші бөлігіне өзгертулер енгізіліп, "соттағы бірыңғай және қосалқы (жылдық) тізімдерден" деген сөздер "соттағы алқабиге кандидаттардың бірыңғай тізімінен" деген сөздермен ауыстырылды [6]. Яғни 2023 жылғы шілде айының бірінші күнінен бастап, алқабиге кандидаттардың бірыңғай тізімінен алқабиге кандидаттарды алдын ала кездейсоқ таңдау жүргізіледі [7].

Алқабилерді іріктеу процесіне Қазақстан Республикасы азаматтарының қатысуын қамтамасыз ету мақсатында алқабилерге кандидаттардың бірыңғай тізімі соттың сұрау салуы бойынша Қазақстан Республикасының ақпараттандыру туралы заңнамасына сәйкес ақпараттандыру саласындағы уәкілетті органның ақпараттық-талдау жүйесі және "электрондық үкіметтің" ақпараттандыру объектілері арқылы электрондық нысанда қалыптастырылады.

Біздің пайымдауымызша аталған сот отырысының күрделігін ескере отырып, алқабилерге кандидаттарды іріктеу процедурасын жеңілдету үшін, оны IT-маманының көмегі арқылы автоматтандыруды қарастыруға болатын шығар, әрине іс бойынша төрағалық етуші судьяның және барлық процеске қатысушылар үшін де жұмыстың біршама жеңілдеуі, уақыттың тиімділігі де орынды болар еді. Оның үстіне автоматты жолмен іріктеуден өткен алқабилердің іс бойынша объективтілігін де қамтамасыз еткен болар ма еді. Ал басты сот талқылауын толықтай, әсіресе сот тергеуін, сот жарыссөзін автоматтандыру екі талай. Десек те, қылмыстық істер бойынша әділеттілікті, ақиқатты электронды таразының орнатуы, ол тағы да уақыттың еншісінде.

Пайдаланылған әдебиеттер тізімі:

1. Мемлекет басшысы Қасым-Жомарт Тоқаевтың Қазақстан халқына Жолдауы 2022 жылғы 16 наурыз. [Электрондық ресурс] - Айналыс режимі: https://www.akorda.kz/kz/memleket-basshysy-kasym-zhomart-tokaevtyn-kazakstan-halkyna-zholdauy-1622340 (жүгінген күні: 08.04.2023).

2. Қазақстан Республикасының Қылмыстық-процестік кодексі Қазақстан Республикасының Кодексі 2014 жылғы 4 шілдедегі № 231-V ҚРЗ. [Электрондық ресурс] - Айналыс режимі: https://adilet.zan.kz/kaz/docs/K1400000231#z2393 (жүгінген күні: 08.04.2023).

3. Қылмыстық сот ісін электрондық форматта жүргізу жөніндегі нұсқаулықты бекіту туралы Қазақстан Республикасы Бас прокурорының 2018 жылғы 3 қаңтардағы № 2 бұйрығы. Қазақстан Республикасының Әділет министрлігінде 2018 жылғы 23

қаңтарда № 16268 болып тіркелді. [Электрондық ресурс] - Айналыс режимі: https://adilet.zan.kz/kaz/docs/V1800016268 (жүгінген күні: 08.04.2023).

4. Қазақстан Республикасының кейбір заңнамалық актілеріне қылмыстық сот ісін жүргізу саласындағы адам құқықтары, жазаны орындау, сондай-ақ азаптау мен басқа да қатыгез, адамгершілікке жатпайтын немесе қадір-қасиетті қорлайтын қарым-қатынас түрлерінің алдын алу мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы Қазақстан Республикасының Заңы 2023 жылғы 17 наурыздағы № 212-VII ҚРЗ [Электрондық ресурс] - Айналыс режимі: https://adilet.zan.kz/kaz/docs/Z2300000212#z73 (жүгінген күні: 08.04.2023).

5. Қазақстан Республикасының Конституциясы 1995 жылы 30 тамызда республикалық референдумда қабылданды. [Электрондық ресурс] - Айналыс режимі: https://adilet.zan.kz/kaz/docs/K950001000_ (жүгінген күні: 08.04.2023).

6. Қазақстан Республикасының Қылмыстық-процестік кодексі Қазақстан Республикасының Кодексі 2014 жылғы 4 шілдедегі № 231-V ҚРЗ. [Электрондық ресурс] - Айналыс режимі: // https://adilet.zan.kz/kaz/docs/K1400000231#z2393 (жүгінген күні 20.04.2023).

7. Қазақстан Республикасының кейбір заңнамалық актілеріне инновацияларды ынталандыру, цифрландыруды, ақпараттық қауіпсіздікті дамыту және білім беру мәселелері бойынша өзгерістер мен толықтырулар енгізу туралы Қазақстан Республикасының Заңы 2022 жылғы 14 шілдедегі № 141-VII ҚРЗ. [Электрондық ресурс] - Айналыс режимі: https://adilet.zan.kz/kaz/docs/Z2200000141#z222 (жүгінген күні: 20.04.2023).

Рахметулин Абай Джамбулович
Судья Верховного Суда Республики Казахстан,
г. Астана, Республика Казахстан

Доклад на тему:

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ОСУЩЕСТВЛЕНИИ ПРАВОСУДИЯ ПО УГОЛОВНЫМ ДЕЛАМ

На протяжении последних лет благодаря стремительному развитию науки и человеческого капитала появилось много информационных технологий, которые могут уже самостоятельно функционировать благодаря использованию и развитию искусственного интеллекта.

Возможности использования искусственного интеллекта в различных направлениях юриспруденции все чаще и чаще обсуждаются как учеными-юристами, так и практиками (судьями, прокурорами, адвокатами, практикующими юристами). Вопросы использования искусственного интеллекта в организации судоустройства в целом, и в уголовном процессе в частности, представляют при этом значительный интерес и исследуются все большим количеством людей, о чем свидетельствует и сегодняшнее мероприятие с участием международных экспертов.

Применение технологий искусственного интеллекта в судопроизводстве потенциально может позволить более эффективно достигать некоторых целей в этой области.

Прежде всего, применение технологий искусственного интеллекта позволит снизить масштабы проблемы доступа населения к правосудию.

Технологии искусственного интеллекта обладают определённым потенциалом для улучшения работы судебных органов, в частности, посредством обеспечения поддержки работы судей.

Искусственный интеллект обладает преобразовательным потенциалом в отношении юридической практики, в частности, в силу того, что компьютеры способны существенно быстрее обрабатывать все данные и владеть большей информацией.

Использование новых технологий в судопроизводстве может способствовать реформированию системы правосудия за счёт использования больших данных, в том числе о взаимодействиях, а также более сложных генерации и интеграции знаний.

Зачастую наиболее ценным вкладом системы искусственного интеллекта является именно анализ основных практических задач и требований к обработке связанной с ними информации.

Кроме того, формирование судебных актов через искусственный интеллект на тех этапах, когда большая часть фактических вопросов уже решена, и решение можно принять посредством лишь оценки

согласованных фактов, может быть более эффективным, прозрачным, последовательным и процессуально экономичным.

Можно выделить следующие преимущества искусственного интеллекта:

1. скорость работы, поскольку обращения в систему правосудия возросло, что делает использование информационных технологий в этой области, необходимостью;

2. объективность, так как будет обеспечена полная беспристрастность, лишённая неуместного сочувствия, восхищения или воздействия иных субъективных чувств при принятии решений;

3. отсутствие математических ошибок при расчётах, которые влияют на суммы взыскания ущерба, определения вида наказания, вида учреждения уголовно-исполнительной системы.

Использование элементов искусственного интеллекта поможет судье, используется исключительно как вспомогательный инструмент, способный совершать определенные действия самостоятельно и выступает помощником судьи.

Искусственный интеллект, наделённый некоторыми функциями судьи, может использоваться для повышения эффективности работы судов и для решения сложных правовых задач, может составлять судебные акты. Такого рода программы могут осуществлять проверку и обеспечение представления надлежащим образом претензий сторон, осуществлять оценку хода дела.

Необходимо отметить следующие возможные направления применения технологий искусственного интеллекта в судопроизводстве:

а) искусственный интеллект может выступать в качестве интеллектуальных помощников для судей аналогично тому, как помогают врачам диагностировать заболевания и рекомендовать лечение;

б) может изучать огромные объёмы информации, определять закономерности, которые человек может пропустить, а также предоставлять необходимые выводы для проведения юридических исследований и анализа;

в) может анализировать ситуации, определять возможные варианты применения законодательства и производить оценку возможных решений (например, в тех случаях, когда факты неоспоримы, применимое законодательство очевидно, а также известны схожие прецеденты, искусственный интеллект может диагностировать ситуацию и разработать проект решения для его рассмотрения судьёй, что может быть полезным при рассмотрении стандартных дел.

Искусственный интеллект, выполняющий функции и полномочия судьи, не подвержен эмоциям, способен строго придерживаться законодательных рамок и выносить решения с учётом многих факторов,

включая данные, которые характеризуют участников спора, сможет оперировать существенно большими (нежели человек) объёмами массивов данных из хранилищ государственных служб, прежде всего – из архивов судебных дел и справочных правовых систем, сможет несопоставимо быстрее обрабатывать данные и учитывать значительно больше факторов.

Хотелось бы отметить, что для успешной реализации потенциала искусственного интеллекта в уголовном процессе и повышения доверия к нему необходимо соответствующее правовое регулирование и определение преимуществ и рисков замены человека компьютером.

Во многих странах работа по разработке нормативно-правовых актов уже давно ведется, а в некоторых странах ряд документов уже разработано. Самым известным из таких документов является «Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях» принятая 4 декабря 2018 г. Европейской комиссией по эффективности правосудия Совета Европы. Это первый принятый в Европейском Союзе нормативный акт, в котором излагаются этические принципы, касающиеся использования искусственного интеллекта в судебных системах, к которым отнесены принцип уважения основных прав и свобод человека, принцип недопустимости дискриминации лиц, принцип качества и безопасности обработки судебных решений и иных баз данных, принцип прозрачности, беспристрастности и справедливости, принцип подконтрольности систем пользователю.

В Китайской народной республике, согласно принятой в 2021 г. дорожной карте, планируется к 2025 г. модернизация судебной системы посредством внедрения, так называемых «умных судов». Данная система на основании технологий искусственного интеллекта сможет анализировать фактические обстоятельства дела, представленные в суд доказательства (документы), и уведомлять судью в случае отступления от формальных требований законодательства (обращать внимание на истечение срока рассмотрения дела, на ошибку в случае выхода за установленные пределы назначаемого наказания). При этом с апреля 2020 г. в десяти шанхайских судах уже применяются технологии по расшифровке аудиозаписей судебных процессов, предоставлению доказательств в цифровом виде и поиску информации в представленных по делу доказательствах.

В Индии система автоматизированных и виртуальных судов рассматривает мелкие правонарушения, связанные с нарушением правил дорожного движения.

В Казахстане, учитывая развитие современных информационных технологий, Верховным Судом прорабатывались возможности использования элементов искусственного интеллекта (технологии «машинного обучения») в вопросах отправления правосудия.

Так, Верховным Судом было создано специальное хранилище окончательных судебных актов и их электронного описания (метаданных) объемом более 5 млн. документов.

На основе этого хранилища были созданы 2 поисковые и аналитические системы с применением технологий больших данных (Big Data) и машинного обучения: сервис «Судебная практика» и аналитическая информационная система «Цифровая аналитика судебной практики».

«Цифровая аналитика судебной практики» позволяет найти любую информацию в тексте, анализируя миллионы состоявшихся судебных актов в один клик. Система демонстрирует, какое количество найденных по конкретному запросу решений обжаловались в апелляции и кассации. Судья видит судебную практику по схожим делам, вплоть до кассации.

Программа обучена понимать судебные решения, сравнивать их между собой, выявлять аномалии и прогнозировать исход рассматриваемого дела. Допустим, судью интересует практика по конкретному иску, который содержит массу аргументов и нюансов. Поисковик автоматически найдет все максимально схожие дела, с результатами их обжалования в вышестоящие инстанции. И еще: программа найдет решения, выбивающиеся из судебной практики, будет сигнализировать об аномалиях и подсказывать, на что нужно обратить внимание и разобраться в причинах резкого отличия.

Однако решения всегда будут принимать сами судьи. Искусственный интеллект значительно упрощает решение их рутиных задач. Анализ искусственного интеллекта может использоваться только как дополнительный инструмент при осуществлении правосудия.

Также роботизирован процесс санкционирования постановлений частных судебных исполнителей об ограничении выезда за рубеж.

Судебные акты составляются ИИ, судья их проверяет и подписывает.

В 2022-м с применением искусственного интеллекта (робот) было зарегистрировано 126 тыс. материалов из поступивших 156 тыс., отклонено 4,7 тыс.

Робот формирует и судебные приказы о взыскании алиментов на несовершеннолетних детей: с марта 2022-го зарегистрировал более 8 тыс. заявлений.

Сейчас анализируются категории дел и материалов с потенциалом для роботизации. Таким образом, с одной стороны, будут обеспечиваться оперативность принятия решений, разгрузка судов от рутины, а с другой - минимизирование судебных ошибок, судьи будут сконцентрированы на рассмотрении сложных дел.

IT-сообщество может пользоваться судебной информацией сервиса на платформе Smart Bridge, через нее возможна разработка собственных аналитических продуктов.

Сервис интегрирован с Ситуационным центром Верховного Суда (СЦ). СЦ нацелен на оперативный мониторинг и анализ работы судов, способствует консолидации показателей деятельности судебной системы на основе актуальных источников информации и созданию эффективной системы управления судебной власти.

СЦ автоматически мониторит и анализирует судопроизводство, делопроизводство, информационную безопасность, применение АВФ и другие показатели. Данные по 850 показателям доступны как в целом по республике, так в разрезе регионов и отдаленных судов. Это позволяет в реальном времени формировать десятки аналитических справок: о соблюдении процессуальных сроков, судебной нагрузке, категориях дел и др.

Вместе с этим предлагаю по уголовному судопроизводству на первоначальном этапе возможно вынесение решения роботом по уголовным проступкам, преступлениям небольшой тяжести, где не оспариваются доказательства, квалификация совершенного уголовного правонарушения и нет альтернативных наказаний. Например, по УПК Казахстана это возможно по делам приказного производства, также по делам ускоренного досудебного расследования и рассмотрения дела.

В свое время работавшая программа – модуль «Помощь судьям» по уголовным делам дала положительный эффект при осуществлении правосудия, ошибки при применении уголовного и уголовно-процессуального законодательства были минимизированы. Искусственный интеллект высчитывал при определенных условиях: когда нельзя больше определенного законом срока назначать наказание, какой вид исправительного учреждения будет правильным назначить осужденному, какой вид рецидива имеется в действиях осужденного и т.д. Считаю необходимым возобновить и совершенствовать указанный модуль.

Также искусственный интеллект можно использовать на стадиях апелляционного и кассационного рассмотрения дел.

Это касается: проверки соблюдения сроков обжалования, опротестования судебных актов, надлежащее ли лицо подало жалобу, ходатайство, протест, если не соблюдены, то автоматически возвращаются, также возможность выдачи данных по судебной практике по категории дел, которые обжалуются, подготовка проекта постановления по результатам рассмотрения, которое после проверки может быть подписано составом коллегии.

Большое значение имеет следующая стадия судопроизводства, это – рассмотрение вопросов, связанных с исполнение приговора (УДО, ЗМН, об изменении вида учреждения уголовно-исполнительной системы и другие вопросы, установленные в УПК. К ним можно отнести все преступления, кроме особо тяжких, террористических, коррупционных и преступлений, совершенных организованной группой.

Искусственный интеллект может обработать срок отбытия наказания и определить подошел ли срок осужденного для УДО, ЗМН, какие имеются характеризующие данные в отношении осужденного, выполнены ли все условия, требования закона для освобождения от наказания или замены на более мягкое наказание.

То есть, робот, проверив все основания, указанные в законе, и установив их соблюдение, может выдать постановление об условно-досрочном освобождении от наказания осужденного лица или о замене на более мягкое наказание. При этом не будет указано в постановлении какие-либо непредусмотренные законом основания для отказа в удовлетворении ходатайства осужденного.

На практике встречаются случаи, когда судьи отказывают в освобождении по непредусмотренным законом основаниям, что исправляется в последующем вышестоящей инстанцией.

Из всего сказанного можно сделать вывод, что применение искусственного интеллекта при осуществлении правосудия разделить на два направления:

1. Искусственный интеллект прорабатывает все критерии от начала поступления дела в суд и выносит окончательное решение.

2. Искусственный интеллект оказывает помощь судье при рассмотрении дела и вынесения правильного судебного акта.

Тем самым мы видим, что потенциал искусственного интеллекта неисчерпаем, главное, чтобы его использование было полезно для общества, особенно учитывая, что при осуществлении правосудия затрагиваются права и свободы граждан, которые не должны быть ущемлены.

Считаю, что сегодняшняя научно-практическая конференция даст импульс в дальнейшем развитии искусственного интеллекта в правоприменении в целом.

УДК 004.8:34

Салиенко Василий Васильевич
Старший преподаватель Кафедры уголовно-правовых дисциплин
юридического факультета Евразийского национального
университета им. Л.Н. Гумилева,
руководитель Экспертного центра университета
г. Астана, Республика Казахстан,

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЮРИДИЧЕСКАЯ ПРОФЕССИЯ

Аннотация. Искусственный интеллект (ИИ) - это способность компьютеров решать задачи, которые ассоциируются с высокоинтеллектуальными возможностями человека. Искусственный интеллект понимает язык, обучается, способен рассуждать и решать проблемы. Общий ИИ включает в себя более широкие возможности применения ИИ, такие как компьютер, обучающий различным задачам и способность решать проблемы, как человек. Новые инструменты ИИ. Автоматизация юридической работы. Искусственный интеллект как атрибут эффективной уголовно-процессуальной деятельности.

Ключевые слова: искусственный интеллект; программирование расследования; компьютеризация расследования; искусственные нейронные сети; криминалистическое мышление.

Аннотация. Жасанды интеллект (AI) - компьютерлердің жоғары интеллектілі адам мүмкіндіктерімен байланысты мәселелерді шешу қабілеті. Жасанды интеллект тілді түсінеді, үйренеді, есептер шығара алады. Жалпы AI әртүрлі тапсырмаларды үйрететін компьютер және адам сияқты мәселелерді шешу мүмкіндігі сияқты AI-ның кеңірек қосымшаларын қамтиды. Жаңа AI құралдары. Құқықтық жұмысты автоматтандыру. Жасанды интеллект тиімді қылмыстық іс жүргізудің атрибуты ретінде.

Түйінді сөздер: жасанды интеллект; тергеуді бағдарламалау; тергеуді компьютерлендіру; жасанды нейрондық желілер; криминалистикалық ойлау.

Annotation. Artificial intelligence (AI) is the ability of computers to solve problems that are associated with highly intelligent human capabilities. Artificial intelligence understands language, learns, is able to reason and solve problems. General AI includes broader applications of AI, such as a computer teaching different tasks and the ability to solve problems like a human. New AI tools. Automation of legal work. Artificial intelligence as an attribute of effective criminal procedure.

Keywords: artificial intelligence; investigation programming; computerization of the investigation; artificial neural networks; criminalistic thinking.

Введение. Машинное обучение — это процесс создания машин или программ, которые могут получать доступ к данным, применять к ним алгоритмы, получать ценную информацию и затем применять полученные знания к другим сценариям или новым наборам данных. Большие данные — топливо ИИ. Это и то, что обучает ИИ, становится все более и более мощным, и то, к чему в конечном итоге применяются системы ИИ, чтобы генерировать реальное понимание, а также это

технологии поиска, обработки и применения неструктурированной информации. Чем больше систем искусственного интеллекта может использовать данные, тем больше их интеллект и разрушительный потенциал [1].

Последние месяцы вполне могут войти в историю как момент, когда прогнозный искусственный интеллект (ИИ) стал мейнстримом (ме́йнстри́м (англ. mainstream — «основное течение») — преобладающее направление в какой-либо области (научной, культурной и других) для определённого отрезка времени. ИИ для создания текста, речи, изображений и видео быстро развивается, что обещает управленцам, торговле и общественной жизни далеко идущие последствия.

Неудивительно, что в этот сектор хлынул поток капитала: правительства и компании инвестируют в стартапы для разработки и развертывания новейших инструментов машинного обучения. Эти новые приложения будут сочетать исторические данные с машинным обучением, обработкой естественного языка и углубленными знаниями по определению вероятности будущих событий. Важно отметить, что внедрение новой обработки естественного языка и генеративного ИИ не будет ограничено богатыми странами и такими компаниями, как Google, Meta и Microsoft, которые возглавили их создание. Как отмечает исследователь технологий Нанджира Самбули, цифровизация имеет тенденцию усугублять, а не решать существующие политические, социальные и экономические проблемы.

Энтузиазм во внедрении прогностических инструментов должен быть уравновешен осознанным и этическим пониманием их предполагаемых и непреднамеренных эффектов. Там, где влияние мощных алгоритмов подвергается сомнению или неизвестно, принцип осторожности предостерегает от их развертывания.

Создание соответствующих рамок потребует достижения консенсуса по основным принципам, которые должны лежать в основе разработки и использования инструментов прогнозирующего ИИ. К счастью, гонка за ИИ привела к возникновению параллельного шквала исследований, инициатив, институтов и сетей по этике. И хотя ведущую роль взяло на себя гражданское общество, к нему присоединились и межправительственные организации, такие как ОЭСР и ЮНЕСКО.

Если новые инструменты ИИ просто импортировать и широко использовать до того, как будут созданы необходимые структуры управления, они легко могут принести больше вреда, чем пользы.

Основная часть. Глобальная гонка по разработке и внедрению новых инструментов прогнозного ИИ нуждается в системах предотвращения вреда для обеспечения безопасного, процветающего, устойчивого и ориентированного на человека будущего.

Сфера юриспруденции, которая до недавних пор являлась

консервативной в области новых технологии, в последнее время претерпевает значительные изменения. Развитие цифровых технологии в юриспруденции можно выделить в нескольких направлениях: автоматизация типовых юридических услуг, юридические онлайн-сервисы для клиентов, переход системы правосудия в онлайн, а также создание решений на основе искусственного интеллекта. Весь доступный инструментарий для юриста сегодня это:

- конструкторы документов, работающие на основе типовых и унифицированных шаблонов, в которых любое отклонение от формы требует ручной правки;
- сервисы проверки контрагента, осуществляющие агрегацию общедоступной информации из публичных реестров (ЕГРЮЛ/ЕГРИП, Федресурс, КАД и др.), которые редко позволяют найти ценную информацию;
- системы подбора судебной практики и справочно-правовые системы, осуществляющие базовый поиск по ключевым словам, фразам, тегам в открытой базе судебных решений и НПА, которые предоставляют все документы, содержащие искомое слово без учета контекста и др.;
- системы управления проектами, задачами и документами (различные BPM/ERP/ECM-системы, заточенные на автоматизацию биллинга, учет времени и контроль за ресурсами).

Данные инструменты ни на шаг не приближают к автоматизации творческой и экспертной юриспруденции. Они, безусловно, облегчают работу юриста, но только в вопросах поиска информации, а не в ее интеллектуальной обработке с точки зрения юридической логики. Практикующие юристы высокой квалификации согласятся с тем, что если бы можно было предлагать клиентам шаблонные договоры, в которые встроены актуальные даты, суммы и наименования объектов, то профессии юриста уже бы не было. Ценность юриста заключается в его способности предвидеть ситуацию на несколько шагов вперед и предлагать нестандартные решения в пользу клиента с минимальными рисками и издержками с точки зрения права.

При существующем уровне развития технологий юридический рынок в Казахстане (и, скорее всего, в мире) не имеет полноценных решений, способных заменить юриста даже начальной квалификации и автоматизировать хоть в сколько-нибудь значимой части юридическую функцию.

Одна из значимых компетенций юриста — это умение видеть в письменных документах все юридические факты, выделять наиболее значимые и соотносить их с нормами права для поиска возможных решений. Именно поэтому одной из ключевых и первостепенных задач, которую необходимо решить для создания действительно функционирующих инструментов автоматизации юридической работы,

является обучение машины смысловому понимаю текста на уровне юриста-профессионала [2]. Речь идет о полноценном семантическом анализе юридических текстов. Без применения глубоких лингвистических технологий решить задачи автоматизации юридической функции и создания полноценного юридического искусственного интеллекта не получится. Это, прежде всего, связано с необходимостью научить программные инструменты понимать не только отдельные сущности (категории) в тексте, но и анализировать текст, выделять все возможные смыслы и проводить логические взаимосвязи в его содержании.

Результаты исследования существующих решений в области процессинга текста привели к выводу, что представленные на рынке инструменты имеют универсальный характер и неприменимы в существующем виде для достижения практических результатов в анализе слабоструктурированных и неструктурированных правовых документов. Причин тому несколько.

Основная проблема, присущая всем представленным решениям, заключается в том, что продукт создан не экспертами предметной области, в которой он применяется. Идея создания инструментов автоматизации юридической работы без участия юристов высокой квалификации изначально обречена на неудачу, поскольку без понимая терминологии, ее значений и классификаций, а также самых глубинных взаимосвязей невозможно воссоздать «юридическую картину мира». Во многом данная ситуация связана с тем, что на рынке доминируют подход, при котором идеологами проектов по созданию решений автоматизации выступают IT-разработчики и специалисты в области data science, которые не знакомы на должном уровне с особенностями юридического мышления и не погружены в реальную практику, в которой может применяться то или иное решение.

Создать высокоэффективное программное решение, которое может быть интегрировано в конкретную предметную область, невозможно без участия экспертов из данной области, профессиональный опыт и логика которых ложатся в основу машинных алгоритмов. Именно поэтому создание «цифрового юриста» (юридического ИИ) и содержательная автоматизация юридической функции:

- возможны только в результате глубинного погружения в предметную область;
- находятся на пересечении 3 различных областей знаний: юриспруденция, лингвистика и IT.

В результате тесного взаимодействия специалистов из этих областей будут созданы новые уникальные для рынка компетенции. Данные компетенции находятся на стыке нескольких областей — юриспруденции, лингвистики, программирования и инженерии знаний,

что приведет к формированию принципиально новых профессий, отсутствие которых сегодня является одним из наиболее существенных факторов, сдерживающих развитие рынка технологий искусственного интеллекта в Казахстане.

Митио Каку в своей книге «Будущее физики» предполагает, что люди, профессии которых связаны с человеческими отношениями, в том числе юристы, не останутся без работы, обосновывая это тем, что «робоюрист сможет ответить на простейшие вопросы по законам и юридической процедуре, но законы постоянно изменяются вместе с социальными стандартами и моралью. В конечном итоге интерпретация закона сводится к ценностной оценке, в которой компьютеры не сильны. Робот не сможет заменить присяжных, потому что те должны представлять здравый смысл и моральные принципы определенной группы людей, а они меняются со временем.»

Для судьи во время отправления им правосудия, такие философско-этические категории как «истина», «добро» и «справедливость» имеют важное значение, поскольку именно эти ценности являются нравственными принципами разумного общества.

Кроме того существует понятие свободы судейского усмотрения, - обязанность суда разрешать спор в соответствии с обстоятельствами дела, применяя социальные нормы, которые являются истинно правовыми, то есть гуманными, защищающими законные интересы личности, т.к. одной из основных задач профессии судьи является реальная помощь человеку имеющимися правовыми средствами.

На основании исследования следует согласиться с точкой зрения Л. Мель («Автоматизация в юридическом мире: от машинной обработки правовой информации до «правовой машины»»), что искусственный интеллект может быть помощником юриста, но не заменой ему. Основной задачей искусственного интеллекта в расследовании преступлений является анализ больших объемов информации с целью выявления сведений, имеющих значение для уголовного дела [3].

Искусственный интеллект, прогрессируя с каждым годом будет выступать атрибутом не только эффективной уголовно-процессуальной деятельности, но и передовых криминалистических методов расследования и раскрытия преступлений, обладающих дополнительными функциями. Однако, следует помнить, что искусственный интеллект является лишь инструментом в руках правоохранительных органов, который не должен вытеснять человека.

Криминалистика всегда отличалась высокой восприимчивостью к технологиям, потенциально полезным в выявлении и раскрытии преступлений, так что рассмотрение перспектив использования искусственного интеллекта представляет для нее большой интерес.

Известный исследователь искусственного интеллекта Дж. Коупленд предлагает два подхода к его пониманию: «нисходящий» (Top-

Down) и «восходящий» (Bottom-Up). В рамках первого подхода речь идет о прикладном моделировании отдельных компонентов (процессов) человеческого мышления в целях решения узкоспециализированных, частных задач. Применительно к вопросам обеспечения деятельности по раскрытию и расследованию преступлений такой подход к пониманию искусственного интеллекта уже активно используется при разработке и внедрении экспертных систем, автоматизированных баз данных и пр. С точки зрения восходящего подхода к пониманию искусственного интеллекта последний предполагает уже полноценное поведение или мышление, т. е. комплексную оценку входящих сообщений и принятие на их основе взвешенных решений в условиях неполной, фрагментированной информации [4].

В практике раскрытия и расследования преступлений активно используются автоматизированные информационно-поисковые системы, позволяющие получать информацию о возможных направлениях расследования:

- автоматизированная баллистическая информационно-поисковая система «Арсенал», обеспечивающая сканирование и ввод в систему высококачественных изображений боковой поверхности пуль и гильз;
- система «Блок», обеспечивающая информационное криминалистическое сопровождение расследования экономических преступлений;
- система «Маньяк», обеспечивающая получение информации при расследовании серийных убийств;
- автоматизированная дактилоскопическая информационно-поисковая система «Папилон», обеспечивающая технологический процесс работы с дактилоскопическими объектами;
- система «Спрут», помогающая установить контактные связи преступников;
- система «Сейф», в которой систематизируется информация о хищениях денежных средств из хранилищ;
- географическая информационная система «Зеркало», оперирующая пространственными (фактографическими и статистическими) данными и др.

Подобные экспертные системы способствуют повышению эффективности управления путем автоматизации деятельности и функционирования правоохранительных органов, позволяют значительно снизить временные затраты на принятие решений в рамках конкретной ситуации, связанной с правом, обеспечивают улучшение качества и проработанности принимаемого решения.

Для целей правовых отраслей знания, в том числе криминалистики, искусственные нейронные сети можно рассматривать как программные или аппаратные комплексы простых обработчиков данных, способных обмениваться друг с другом сигналами и при

достаточно развитой структуре и настроенной логике взаимодействия решать сложные задачи. Специфику искусственных нейронных сетей обусловливают простота каждого их элемента (искусственного нейрона), их взаимозаменяемость и взаимосвязь. Каждый кластер информации, загружаемый в сеть, сопоставляется с другими кластерам, на основе чего генерируется решение задачи. Рабочая искусственная сеть может содержать десятки и сотни слоев (уровней оценки и проверки), обеспечивающих комплексное рассмотрение любых факторов, что позволяет решать крайне сложные задачи, в том числе по раскрытию и расследованию преступлений.

Работа искусственной нейронной сети основана на интеллектуальном эвристическом анализе данных, который гораздо более эффективен, чем методы математической статистики, используемые в большинстве криминалистических программных комплексов. В этом отношении искусственные нейронные сети гораздо ближе к человеческому мозгу, поскольку способны выявлять скрытые, неочевидные связи и закономерности, подобно тому как талантливый следователь может связать в единую картину разрозненные обстоятельства совершения преступления, известные следствию.

Основные направления, где могут быть использованы искусственные нейронные сети:

1. Оценка исходной информации по уголовному делу в целях выдвижения простых и комплексных следственных версий, определение направлений их проверки.

2. Моделирование события преступления и его следовой картины на основе неполных данных и предшествующего «опыта», охватывающего большой массив уголовных дел.

3. Выявление признаков серийности в условиях информационной недостаточности и предложение вариантов действий следователя по проверке перспективных следственных версий.

4. Увеличение эффективности почерковедческих и габитоскопических исследований: к настоящему времени наиболее перспективным направлением развития искусственных нейронных сетей считается распознавание образов, что может позволить, к примеру, автоматизацию выявления признаков подлога документов.

5. Поиск недоступных криминалистическому программному обеспечению компьютерных файлов, сокрытых, например, при помощи стеганографии или альтернативных потоков данных (ЛОЗ), установление первичного источника информации в сети Интернет.

Хотя искусственный интеллект по сути не является алгоритмизированным (в силу отсутствия заданной последовательности шагов), он может выступить важным помощником следователя. Однако любые типы искусственного интеллекта, которые могут быть использованы при раскрытии и расследовании преступлений, должны

быть апробированы, а сама возможность их применения - закреплена в уголовно-процессуальном законодательстве.

Искусственные нейронные сети могут быть адаптированы для решения специфических криминалистических задач, например анализа материалов уголовных дел для выявления следственных ошибок процессуального и тактического характера, вычленения из массива расследуемых дел признаков серийности, объединения преступлений по схожим признакам [5]. В ближайшем будущем вполне возможна интеграция рассмотренной технологии в криминалистическую практику, однако для этого требуется дальнейшее изучение архитектуры и возможностей искусственных нейронных сетей, в том числе учеными-криминалистами.

Заключение. ИИ никогда не заменит высококвалифицированного, опытного эксперта по идентификации. Но нейросеть может помочь в работе менее опытным специалистам в идентификации, и таким образом снять часть нагрузки с экспертов, чтобы они смогли сосредоточиться на действительно сложных в расследовании делах.

Как видно, технологии начинают менять работу юристов и уже способны заменить их в некоторых отраслях. Так, на сегодняшний день успешно работают чат-боты, способные оспорить штраф за неправильную парковку, помочь с составлением юридических документов или речи для судебного заседания. Стремительное развитие технологий действительно может оставить не у дел многих юристов, в частности тех, чья работа связана с выполнением несложных повторяющихся действий. Вместе с тем пока преждевременно говорить об их полной замене машинами. Так, неправильное обучение ИИ может привести, например, к расовой дискриминации или предвзятости. Кроме того, роботы пока не могут проявлять сочувствие, «слушать собеседника» и проявлять терпимость – чувства, за которыми зачастую люди и обращаются к юристам. Несмотря на имеющиеся недостатки, использование технологий может заметно снизить текущую нагрузку на судебную систему и удешевить предоставление юридических услуг.

Список использованных источников:

1. Пилецкая, А.В. Искусственный интеллект и большие данные (А.В. Пилецкая. — Текст: непосредственный // Молодой ученый. — 2019. — № 50 (288). — С. 20-22. — URL: https://moluch.ru/archive/288/65241/ (дата обращения: 17.04.2023)

2.Амиянц К.А. Использование искусственного интеллекта в современной судебной системе и права человека;

3. Винтер М.Е. Искусственный интеллект в криминалистической науке;

4. Стукалин И.В. Некоторые аспекты использования искусственного интеллекта при производстве криминалистических экспертиз;

5. Трущенков И.В. Использование технологий искусственного интеллекта в криминалистике и судебной экспертизе.

УДК 343.11:004

Синкевич Вероника Викторовна
Доцент кафедры уголовного процесса учебно-научного комплекса по предварительному следствию в органах внутренних дел Волгоградской академии МВД России, кандидат юридических наук, полковник полиции, г. Волгоград, Российская Федерация

К ВОПРОСУ О СТАНОВЛЕНИИ ЦИФРОВОЙ ЭПОХИ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Аннотация. В научной статье обозначена актуальность тематики, связанной с цифровизацией правосудия и уголовного судопроизводства, в частности, как с учетом российского, так и зарубежного опыта, а также в условиях усиления значимости интеграции технологий в правовое поле. В работе рассматриваются вопросы свершившихся апробаций внедрения тех или иных технических средств в уголовном процессе, их применение и использование в практической деятельности должностных лиц и органов. Также в статье говорится о существующих проблемах применения цифровых технологий в судопроизводстве и тенденциях дальнейшего их вживления в процессуальную деятельность.
Ключевые слова: уголовный процесс; цифровизация; правосудие; электронное уголовное дело; цифровые технологии; формат уголовного дела; электронный документ.

Аннотация. Ғылыми мақалада сот төрелігі мен қылмыстық сот ісін цифрландырумен байланысты тақырыптың өзектілігі, атап айтқанда ресейлік және шетелдік тәжірибені ескере отырып, сондай-ақ технологияларды құқықтық салаға интеграциялаудың маңыздылығын күшейту жағдайында көрсетілген. Жұмыста қылмыстық процеске белгілі бір техникалық құралдарды енгізуге, оларды қолдануға және лауазымды адамдар мен органдардың практикалық қызметінде қолдануға қатысты апробация мәселелері қарастырылады. Сондай-ақ, мақалада сот ісін жүргізуде цифрлық технологияларды қолданудың қазіргі проблемалары және оларды іс жүргізу қызметіне одан әрі енгізу тенденциялары туралы айтылады.
Түйінді сөздер: қылмыстық процесс; цифрландыру; сот төрелігі; электрондық қылмыстық іс; цифрлық технологиялар; қылмыстық іс форматы; электрондық құжат.

Annotation. The relevance of the topic related to the digitalization of justice and criminal proceedings is shown in the scientific article, in particular, taking into account Russian and foreign experience, as well as in the context of strengthening the importance of integrating technologies into the legal sphere. The work examines the issues of approbation regarding the introduction of certain technical means in criminal proceedings, their use in the practical activities of officials and bodies. The article also discusses the current problems of using digital technologies in legal proceedings and trends in their further introduction into procedural activities.
Keywords: criminal process; digitalization; justice; electronic criminal case; digital technologies; format of criminal case; electronic document.

В современном мире нет ничего более привычного обществу и государству как наблюдение *набравшей* обороты трансформации всех

сфер жизни в призме применения цифровых технологий. Кажется, что не остается уже ни одного поля деятельности, куда бы не проникли, не внедрились новейшие цифровые разработки, позволяющие жить, работать, обучаться, отдыхать иначе, по-новому. В зависимости от возрастной группы, от полученной профессии, уровня интеллекта и т.д. каждый человек по-своему оценивает интегрирование новейших технологий в ту или иную сферу жизни, однако нельзя не признавать тот факт, что эти изменения произошли, они глобальные и требуют постоянного *прогресса* общества в данном направлении; «цифровизационный поток» стремителен в своем развитии и заставляет подстраиваться и прогрессировать. Трансформацию *традиционной* формы осуществления той или иной деятельности в электронную форму мы наблюдаем не только в нашей стране, но и во всем мире. *Многочисленные* различного рода представительские мероприятия на данную тематику, задачами которых первостепенно обозначается поиск новых решений по вопросам применения цифровых «помощников», "технологий" нивелировании существующих рисков, разработка более новых технических средств и т.д. Форум Digital almaty: тотальная цифровизация, проводимый в апреле 2023 в Казахстане, II Форум кибербезопасности государства «ЦИФРОТЕХ», X федеральный форум по цифровизации городской среды, Smart city & Region: технологии, безопасность, экология, проводимые и планируемые в России яркое тому подтверждение.

Безусловно, правовая сфера в общем и правосудие, в частности, не является исключением для внедрения цифровых технологий. Руководство высших судов России и ряда других стран неоднократно указывали на положительный опыт цифровизации и необходимость дальнейшего развития применения тех или иных технологий при осуществлении деятельности, связанной как с расследованием преступлений, так и с рассмотрением уголовных дел судами. На X Всероссийском Съезде судей Российской Федерации председатель Верховного Суда РФ Вячеслав Михайлович Лебедев говорил о сформировавшемся опыте применения судами различных технических средств, а также интеграции новейших сервисов. Так, с 2024 года планируется полноценное использование единого сетевого издания судебной системы Российской Федерации – мультимедийного ресурса «Правосудие РФ», который был зарегистрирован Роскомнадзором Российской Федерации 26 апреля 2022 года, благодаря которому еще более повысится уровень электронного правосудия путем внедрения систем дистанционной подачи и получения судебных документов, а также дистанционного участия в судебном процессе. Указанный ресурс призван выполнять и просветительскую функцию: разъяснять гражданам особенности взаимодействия с судами, возможности по защите своих прав, порядок применения примирительных процедур и т.д. В

настоящее время во всех видах судопроизводства уже реализуется возможность подачи процессуальных документов в электронном формате проведения судебных заседаний с использованием видео-конференцсвязи, веб-конференций. Расширение суперсервиса «Правосудие РФ» предусматривает использование судами технологий искусственного интеллекта [1].

Первый заместитель председателя Верховного Суда Республики Беларусь Валерий Калинкович в одном из интервью от 15 апреля 2023 года по случаю столетия Верховного Суда Республики Беларусь также указал на процесс активной цифровизации правосудия в Республике Беларусь, который начался в 2015 году с разработки единой информационной системы судов общей юрисдикции и создания электронной системы общего и судебного делопроизводства, что позволило облегчить «учетную политику» и формирование судебной статистики, развить сервисы электронного извещения участников процесса о времени и месте судебного заседания с учетом различных средств электронной связи. В настоящее время внедрена и действует система аудио- и видео протоколирования хода судебных заседаний. Ведется работа по дальнейшему активному внедрению технологий в судопроизводство, и самая главная задача превратить компьютерную систему в достаточно умного помощника судьи [2].

Сегодняшнее время есть время становления цифровой эпохи, некий переломный этап, в рамках которого происходит смена формы жизни. В ходе одной из международных конференций, посвященной использованию искусственного интеллекта, Президент России Владимир Владимирович Путин подчеркнул важность цифровой трансформации всей страны и определил стратегию ее развития [3]. В настоящее время действует и Указ Президента Российской Федерации от 07.05.2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года», которым установлены приоритетные задачи по цифровизации различных сфер жизни Российской Федерации: создание системы правового регулирования цифрового пространства, подготовку высококвалифицированных специалистов, обеспечение информационной безопасности, использование в основном отечественных разработок передачи, обработки, хранения информации и т.д. [4].

Такой сложный процесс как цифровизация, безусловно, окажет и уже оказывает существенное влияние на уголовное судопроизводство. При этом на настоящий момент кардинальной трансформации процессуальной формы не произошло, однако уже активно используются возможности электронного документооборота, применение видеоконференцсвязи, разработанные сервисы для служебной деятельности и взаимодействия, цифровые средства собирания доказательств. Суть цифровизации уголовного судопроизводства по праву считается разработка проекта

закона о ведении электронного уголовного дела и апробация такой процессуальной деятельности на практике. Во многих странах соответствующий опыт уже имеется. Например, уголовно-процессуальный закон Республики Казахстан (далее УПК РК) содержит статью 42.1, закрепляющую форматы уголовного судопроизводства, предусматривая право субъекта расследования избрать бумажный и (или) электронный вариант оформления. Решение о формате уголовного процесса принимает следователь с учетом мнения участников уголовного процесса и возможностей технического оснащения. Решение принимается в виде постановления. В соответствующем постановлении отражается и принятое следователем решение в случае смены формата уголовного судопроизводства. Избранный формат (электронный или бумажный) видоизменяется в зависимости от фактических обстоятельств. Ч. 3 ст. 42.1 УПК РК предусматривает и частично бумажный формат, разрешая следователю согласовывать с прокурором свои решения и уведомлять его об их принятии, используя возможности электронного документооборота [3, С. 133-134]. Многие другие страны также внедрили и активно используют возможность расследовать преступления не в бумажном, а в электронном формате.

В Германии судопроизводство предполагает и вовсе преимущественно электронный формат, который может быть сменен на бумажную форму только в случае отсутствия технической возможности изготовления электронного документа. Уголовное дело в виде электронного досье формируется из оформленных в виде цифровых файлов процессуальных решений и таких же оцифрованных доказательств.

Прогресс в этом направлении отмечается и в США, Канаде, Швеции, Китае, Дании, Нидерландах, Бельгии, Грузии и ряде других стран.

В своих работах ранее мы уже отмечали, что назрела необходимость более существенных изменений уголовного процессуального закона в части интеграции электронного уголовного дела. Следует рассмотреть возможность о внесении в ст. 5 УПК РФ таких понятий как электронный документ, используемые серверы, электронный носитель информации, формат уголовного дела, электронное уголовное дело, а также иные термины, которые будут применяться при ведении электронного уголовного дела. Главу, регламентирующую общие условия предварительного расследования, стоит дополнить нормой о формате, или внешнем виде уголовного дела, предусмотрев возможность его ведения, как в бумажной, так и в электронном выражении [4].

Процессуалисты в последнее время достаточно часто анализируют тенденции цифровизации уголовного процесса, и мнения ученых схожи

в том, что дальнейший процесс диджитализации уголовного судопроизводства коснется использования доказательств, основанных на использовании технических средств, появлении новых и видоизменений закрепленных УПК РФ следственных действий, оптимизации взаимодействий правоохранительных органов, участников уголовно-процессуальных правоотношений, организациями, применения математических формул и моделей для изучения, прогнозирования преступлений и их расследования [5, С.5]. В числе основных более отдаленных тенденций цифровизации, думается, трансформация процессуальной формы осуществления уголовно-процессуальной деятельности.

В свете уже свершившихся и будущих изменений, безусловно, стоит задуматься об успешном разрешении задач, порожденных необходимостью идти в ногу со временем. Это включает в себя разработку соответствующих нормативных правовых актов, соответствующее материально-техническое оснащение, повышение квалификации правоприменителей, профессорско-преподавательского состава, а также выпускающих специалистов в области права, соблюдение баланса помощи/подмены искусственного интеллекта, следование принципам правосудия в призме общедоступности возможности участия в судопроизводстве, обеспечения прав участников уголовного процесса. Вот часть проблем, которые должны решаться в темпе аналогичном скорости развития цифровых технологий. Однако, не смотря на существующие проблемы, сегодня мы смело можем говорить об эволюции уголовного процесса именно в условиях цифровизации.

Список использованных источников:

1. X Всероссийский Съезд судей Российской Федерации // [Электронный ресурс] – Режим доступа: https://supcourt.ru/press_center/news/31816/ (дата обращения: 22.04.2023 г.).

2. Интервью первого заместителя председателя Верховного Суда Республики Беларусь Валерия Калинковича // [Электронный ресурс] – Режим доступа: https://pravo.by/novosti/novosti-pravo-by/2023/april/73886/ (дата обращения: 22.04.2023 г.).

3. Указ Президента Российской Федерации от 07.05.2018 г. № 204. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года. // [Электронный ресурс] – Режим доступа: http://www.kremlin.ru/acts/bank/43027/page/1 (дата обращения: 22.04.2023 г.).

4. Синкевич В.В. Цифровизация уголовного процесса: зарубежный и отечественный опыт / В.В. Синкевич // Вестник Волгоградской академии МВД России. – 2022. – № 1(60). – С. 133-134. – DOI 10.25724/VAMVD.ZEFG. – EDN MFAABF.

5. Ануфриева, Е.А. Основные направления цифровизации уголовного процесса в России / Е.А. Ануфриева, Т.В. Омельченко // Проблемы получения и использования доказательственной и криминалистически значимой информации: материалы Международной научно-практической конференции, Мисхор (Большая Ялта), 26–27 сентября 2019 года. – Мисхор (Большая Ялта): Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2019. – С. 4-5. – EDN BYJYLI.

Таран Сергей Дмитриевич
Заместитель директора РФЦСЭ при Министерстве юстиции Российской Федерации, кандидат технических наук, старший советник юстиции,
г. Москва, Российская Федерация

доклад на тему:

ЦИФРОВОЙ РУБЛЬ КАК НОВЫЙ ОБЪЕКТ СУДЕБНОЙ ЭКСПЕРТИЗЫ

Тема использования искусственного интеллекта (ИИ) и больших данных на страже правопорядка вызывает все больший интерес в современном обществе.

Развитие технологий в области применения ИИ и сбора больших данных предоставляет правоохранительным органам новые возможности для эффективной борьбы с преступностью, обеспечения безопасности общества и предотвращения преступлений.

В своем выступлении я затрону несколько аспектов использования ИИ и больших данных в правоохранительной деятельности.

Во-первых, анализ больших данных позволяет правоохранительным органам выявлять и анализировать образцы и тенденции преступности. Системы ИИ могут обрабатывать и анализировать большие объемы информации, включая различные по природе данные о преступлениях - социальные медиа, видеозаписи, фотографии и т.д. Это помогает выявлять **скрытые** связи между преступниками, обнаруживать паттерны и предоставлять ценные данные для проведения расследования. Например, системы анализа данных могут выявлять географические области с высоким риском преступности, что позволяет правоохранительным органам сосредоточить ресурсы на этих территориях и принять проактивные меры для предотвращения преступлений.

Во-вторых, использование ИИ и алгоритмов машинного обучения позволяет автоматизировать рутинные процессы, процессы анализа данных и выявления преступлений. Автоматизация позволяет ускорить процесс обработки информации и сократить время реакции на преступления. Например, системы видеонаблюдения с функциями распознавания лиц и поведения могут автоматически определять подозрительные действия и отправлять предупреждения правоохранительным органам. Это улучшает оперативность работы полиции и помогает предотвратить преступления в реальном времени.

Тем не менее, необходимо учитывать и этические аспекты при использовании ИИ и больших данных в правоохранительной сфере. Сбор, хранение и анализ данных должны быть осуществлены в рамках законов о защите приватности и персональных данных

Правоохранительные органы должны строго следить за тем, чтобы использование ИИ не приводило к произволу, дискриминации или. нарушению личного пространства. Аналитические алгоритмы должны быть обучены на объективных данных, чтобы избежать предвзятости и некорректных выводов.

Важно уделять внимание вопросам прозрачности и ответственности. Решения, принимаемые на основе анализа данных и применения ИИ, должны быть объяснимыми и поддающимися проверке.

ИИ может быть использован для преобразования правоохранительной деятельности в целом. Например, анализ данных может помочь выявить тенденции преступности и предсказать возможные области, требующие повышенного внимания в будущем. Это позволит правоохранительным органам эффективно распределить ресурсы и разработать стратегии, направленные на снижение преступности в долгосрочной перспективе.

Не следует забывать о роли человеческого фактора. Искусственный интеллект может быть мощным инструментом, но окончательные решения всегда должны приниматься людьми. Экспертные знания, профессиональный анализ и моральные убеждения необходимы для принятия важных решений, особенно в сложных делах экономической преступности. Искусственный интеллект должен служить поддержкой и помощником для человека, расширяя его возможности и улучшая эффективность работы.

Использование искусственного интеллекта и анализ больших данных на страже правопорядка в сфере предотвращения экономических преступлений открывает новые горизонты. Он предоставляет возможности для раннего выявления преступлений, анализа сложных финансовых транзакций и принятия эффективных мер по предотвращению и расследованию преступлений экономической направленности. Это актуально при анализе хозяйственных операций с использование цифровых и криптовалют.

В фокусе последних новостей о введении в обращение ЦИФРОВОГО рубля актуальным станет вопрос применения технологий ИИ при проведении судебно-экономических экспертиз. Экспертам РФЦСЭ при Минюсте России наряду с разработкой методик проведения подобного рода экспертиз предстоит анализировать огромное количество информации по цифровым следам, транзакциям, другим цифровым признакам и прочим массивам для формирования экспертной оценки. Интеллектуальные системы поддержки принятия решений безусловно облегчат поиск требуемой информации, а набор со временем статистических данных по проведенным экспертизам позволит выявить взаимосвязи в деятельности экспертов. Т.е. зависимость экспертных заключений от заявителей, экспертов, сроков проведения экспертиз. Анализ текстов экспертных заключений также

может выявить зависимости от входных данных. Применение технологии блокчейна может сделать доверительным документооборот между лабораториями.

Так же можно сказать и про лингвистические экспертизы, про религиоведческие. В настоящее время наблюдается беспрецедентный масштаб информационной войны

Это проявляется в непрекращающемся воздействии на гражданское население России, власти и Вооружённые Силы посредством распространения специально отобранной и подготовленной информации, информационных материалов, содержащих заведомо ложную информацию, искажающую реальное положение дел, а также материалов, направленных на разрушение традиционных духовных ценностей, навязывание инородных духовных ценностей, искажение и умаление исторической памяти народа.

Обработка огромных массивов информации и выявление связей между ними – вот где поможет искусственный интеллект.

На 11 Петербургском юридическом форуме, проходившем на прошлой неделе, на стенде РФЦСЭ были продемонстрированы экспертизы драгоценных камней и металлов.

Создание динамической базы данных драгоценных камней и драгоценных металлов совместно с базой данных экспертных исследований с применением искусственного интеллекта позволит с высокой долей вероятности производить оценку качества и стоимости драгоценных камней, металлов, изделий из них, повысить уровень надежности данных, а также регулировать качество экспертизы и оказать помощь в судопроизводстве.

Данный подход также подразумевает непрерывное обновление базы и внесение в нее данных постоянно развивающихся современных исследований, что обеспечит полноту и надежность данных.

На основании анализа большого числа исследований, занесенных в экспертную базу данных, ИИ сможет вычислять определенные закономерности, выявлять свойства драгоценных камней и минералов, что существенно облегчит диагностику и позволит точнее и быстрее проводить экспертизы, а также позволит исключить ошибки эксперта.

Создание такой системы позволит определить происхождение исследуемого материала и обеспечить контроль перемещения драгоценных камней.

Создание автоматизированной системы, повышающей надежность и безопасность интерпретации данных комплексных лабораторных исследований, не исключающей оценки опытного эксперта, существенно ускорит процесс производства экспертизы как при оценке стоимости, так и при оценке качества камней.

Анализ и сравнение данных экспертиз и исследований, проводимых ранее, и данных современных передовых исследований,

уточнение параметров оценки и определения состава позволит усовершенствовать имеющиеся критерии отнесения камней к тому или иному виду/классу и внести соответствующие уточнения в определение понятия драгоценный камень. Это позволит унифицировать отнесение камней к категории драгоценных и повысить надежность и достоверность проводимых экспертиз.

Еще одним преимуществом создания базы данных и применения ИИ может стать обеспечение проведения беспристрастных и независимых экспертиз, устранение внесения подложных данных. Такая система позволит создать единую доверительную систему как в обмене данными исследований между лабораториями, так и систему документооборота, и, главное, создать единый подход к диагностике драгоценных камней.

В заключение хочу выразить уверенность в осмысленном выборе «в помощники» современные технологии, позволяющие в значительной мере расширить границы наших возможностей в анализе, прогнозировании и поддержке принятия решений в таких особенных областях нашей деятельности, каковой является правоохранительная система.

УДК 340.01:004.8

Шульгин Евгений Петрович
Начальник кафедры кибербезопасности и информационных технологий Карагандинской академии МВД Республики Казахстан имени Баримбека Бейсенова,
кандидат юридических наук, майор полиции
г. Караганда, Республика Казахстан

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОПТИМИЗАЦИИ ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЫ

Аннотация. Статья рассматривает роль искусственного интеллекта в оптимизации правоохранительной системы. Анализируются возможности применения этих технологий для повышения эффективности работы правоохранительных органов, а также обсуждаются ряд вызовов, связанных с использованием данных технологий. В статье представлены примеры успешных применений искусственного интеллекта в правоохранительной сфере, а также описаны потенциальные направления развития этих технологий в будущем. В целом, статья имеет практическую значимость для всех заинтересованных сторон, которые стремятся оптимизировать работу правоохранительных органов.
Ключевые слова: искусственный интеллект; правоохранительная деятельность; оптимизация; совершенствование; органы внутренних дел.

Аннотация. Мақала құқық қорғау жүйесін оңтайландырудағы жасанды интеллекттің рөлін қарастырады. Құқық қорғау органдары қызметінің тиімділігін арттыру үшін осы технологияларды пайдалану мүмкіндіктері талданып, осы технологияларды қолданумен байланысты бірқатар мәселелер талқыланады. Мақалада жасанды интеллектті құқық қорғау органдарында сәтті қолдану мысалдары келтірілген, сондай-ақ болашақта осы технологияларды дамытудың әлеуетті бағыттары сипатталған. Жалпы, мақаланың құқық қорғау органдарының жұмысын оңтайландыруға ұмтылатын барлық мүдделі тараптар үшін практикалық маңызы бар.
Түйінді сөздер: жасанды интеллект; құқық қорғау; оңтайландыру; жетілдіру; ішкі істер органдары.

Annotation. This article examines the role of artificial intelligence in optimizing the law enforcement system. The possibilities of using these technologies to improve the efficiency of law enforcement agencies are analyzed, and a number of challenges associated with the use of these technologies are discussed. The article presents examples of successful applications of artificial intelligence in law enforcement, as well as describes the potential directions for the development of these technologies in the future. In general, the article is of practical importance for all stakeholders who seek to optimize the work of law enforcement agencies.
Keywords: artificial intelligence; law enforcement; optimization; improvement; internal affairs bodies.

Введение. В современном мире, где объемы информации постоянно увеличиваются, правоохранительным органам необходимо

иметь доступ к большим данным, чтобы эффективно бороться с преступностью. Однако, объемы информации настолько велики, что их обработка и анализ с использованием традиционных методов может быть чрезвычайно сложной и дорогостоящей. В связи с этим, искусственный интеллект стал ключевой технологией, которая помогает правоохранительным органам извлекать ценные знания из больших объемов данных.

Основная часть. Правоохранительные органы являются ключевым элементом правового государства. Они отвечают за обеспечение безопасности граждан, борьбу с преступностью и соблюдение закона. В современном мире правоохранительные органы сталкиваются с рядом вызовов и задач, которые требуют от них использования новых технологий и подходов. Одной из таких технологий является искусственный интеллект.

По мнению Д.В. Степанова, искусственный интеллект, как и естественный интеллект, – неотъемлемое свойство соответствующей технологии искусственного интеллекта, робота, юнита или программного обеспечения, позволяющего действовать автономно и даже независимо от воли его создателей или правообладателей [1, с. 101]. М.Ю. Канеев и С.А. Махин уточняет, что искусственный интеллект как новая отрасль научного знания берет свое начало в середине XX века. Данный термин «artificial intelligence» (искуственный интеллект) впервые был предложен в 1956 г. на семинаре в Станфордском университете США [2, с. 30].

Искусственный интеллект широко применяется в различных областях, таких как медицина, финансы, производство, образование и другие. Например, в медицине искусственный интеллект может использоваться для диагностики заболеваний, прогнозирования результатов лечения и разработки индивидуальных планов лечения для пациентов. В финансовой отрасли искусственный интеллект может помочь в анализе рынка, прогнозировании изменений цен и управлении инвестициями.

Одним из ключевых элементов искусственного интеллекта является машинное обучение. Машинное обучение представляет собой процесс, в результате которого машина обучается на основе данных, чтобы выполнять определенные задачи. Например, машинное обучение может использоваться для распознавания речи, классификации изображений, предсказания тенденций и других задач.

Еще одной важной областью искусственного интеллекта является глубокое обучение, которое является подмножеством машинного обучения. Глубокое обучение использует нейронные сети для анализа данных и обучения машин. Например, глубокое обучение может использоваться для распознавания речи, классификации изображений и других задач, требующих высокой точности.

Искусственный интеллект также широко применяется в робототехнике. Роботы, оснащенные искусственным интеллектом, могут выполнять различные задачи, такие как сбор данных, монтаж и сборка изделий, инспекция и тестирование и другие.

Однако не стоит забывать, что использование искусственного интеллекта может быть сопряжено с рисками и вызовами. Например, при использовании машинного обучения и глубокого обучения может возникать риск ошибочных результатов. Кроме того, искусственный интеллект может привести к сокращению рабочих мест, что может оказать негативное влияние на экономию и общество.

Также важным аспектом использования искусственного интеллекта является безопасность. Искусственный интеллект может быть подвержен кибератакам и взлому, что может привести к утечке данных и другим проблемам. Кроме того, использование искусственного интеллекта в правоохранительных органах может вызвать опасения в отношении конфиденциальности и прав человека.

Однако, несмотря на вызовы и риски, искусственный интеллект имеет потенциал для оптимизации и улучшения различных сфер жизни, включая правоохранительные органы.

Искусственный интеллект может быть использован в правоохранительных органах для улучшения эффективности и точности работы [3, с. 327]. Например, его можно использовать для автоматической обработки больших объемов данных, включая анализ видео и аудио, анализ текста и других источников информации. Это может помочь правоохранительным органам быстрее и точнее выявлять и предотвращать преступления.

Использование искусственного интеллекта также может помочь в снижении затрат и повышении эффективности работы правоохранительных органов. Например, автоматизация процессов позволит сократить количество ручной работы и увеличить производительность. Также искусственный интеллект может помочь в определении оптимального распределения ресурсов, таких как автомобили и сотрудники, для более эффективной работы. Н.К. Мезвришвили совершенно справедливо указывает на то, что искусственный интеллект создается в первую очередь для достижения крупных целей, таких как управление экономикой, а не для поэтического или музыкального творчества, являющегося сопутствующим видом деятельности. Чем сложнее объект управления, тем сложнее система управления и тем выше риски [4, с. 101].

В этой связи не стоит забывать и про оборотную сторону, при использовании искусственного интеллекта в правоохранительных органах необходимо учитывать риски и вызовы. Например, его использование для профилирования подозреваемых может привести

к дискриминации и нарушению прав человека. Кроме того, искусственный интеллект может быть использован для массового наблюдения, что может привести к нарушению конфиденциальности граждан.

Так, профилирование подозреваемых с использованием искусственного интеллекта может стать серьезной проблемой для общества. С одной стороны, это может быть полезным инструментом для правоохранительных органов, которые ищут способы борьбы с преступностью и защиты общества. Однако, с другой стороны, это может привести к дискриминации и нарушению прав человека, если не используются соответствующие правила и методы.

Профилирование подозреваемых с помощью искусственного интеллекта основано на анализе данных, которые собираются о человеке, включая его личную информацию, привычки, поведение и т.д. Эти данные затем используются для создания профиля, который может указывать на потенциальных преступников. Однако, если такой процесс производится без должного контроля, то это может привести к дискриминации и нарушению прав человека.

В процессе профилирования подозреваемых, искусственный интеллект может использовать предвзятые алгоритмы и данные, которые могут отражать стереотипы, связанные с расой, полом, возрастом и другими личными характеристиками. Это может привести к тому, что люди будут ошибочно определены как потенциальные преступники, просто потому, что они попадают в какие-то определенные группы.

Кроме того, использование искусственного интеллекта для профилирования подозреваемых может привести к массовому наблюдению, что может нарушить конфиденциальность граждан. Если данные, собранные в процессе профилирования, будут использоваться для массового наблюдения, то это может привести к нарушению прав человека на конфиденциальность, что может привести к репрессиям, незаконному задержанию и т.д.

Поэтому, для того чтобы избежать дискриминации и нарушения прав человека в процессе профилирования подозреваемых, необходимо использовать соответствующие методы и правила. В частности, необходимо обеспечить прозрачность и ответственность в процессе сбора и использования данных, а также использовать более объективные алгоритмы и данные, чтобы избежать предвзятости. Также необходимо обеспечить надлежащую защиту конфиденциальности граждан при использовании и обработке их личных данных.

Для того чтобы избежать массового наблюдения, необходимо ограничивать использование искусственного интеллекта для профилирования только в тех случаях, когда это действительно

необходимо для борьбы с преступностью и обеспечения безопасности общества. Кроме того, необходимо установить ясные правила использования и обработки данных, а также проводить регулярные проверки, чтобы убедиться, что правила соблюдаются.

Также следует учитывать, что использование искусственного интеллекта в процессе профилирования подозреваемых может быть только одним из инструментов, а не единственным. Важно не полагаться исключительно на алгоритмы и данные, а также учитывать другие факторы, такие как контекст, обстоятельства и дополнительную информацию, которые могут помочь сделать более точные выводы [5, с. 189].

В целом, использование искусственного интеллекта для профилирования подозреваемых может быть полезным инструментом для борьбы с преступностью и обеспечения безопасности общества. Однако, для того чтобы избежать дискриминации, нарушения прав человека и конфиденциальности граждан, необходимо использовать соответствующие методы и правила, а также учитывать другие факторы, которые могут помочь сделать более точные выводы.

Как следствие, в настоящее время мы находимся в периоде информационной эпохи, который характеризуется увеличением количества информации и скорости ее передачи. Вместе с тем, растет функциональность устройств для хранения и передачи данных. Цифровизация затрагивает различные сферы деятельности и активно развивается, внедряя технологии, которые еще несколько лет назад были невообразимы для большинства людей [6, с. 22].

Заключение. Использование искусственного интеллекта в правоохранительной системе может оптимизировать ее работу, но так же может привести к нарушению прав и свобод граждан. Поэтому, необходимо тщательно оценивать и контролировать его использование в правоохранительных органах и разрабатывать соответствующие правовые и этические принципы использования. Кроме того, следует обучать сотрудников правоохранительных органов основам работы с искусственным интеллектом и основам этики при его использовании в работе. Интеграция искусственного интеллекта в правоохранительную систему должна быть осуществлена с соблюдением принципов прозрачности, ответственности и учета мнения граждан. Это означает, что правоохранительные органы должны четко объяснять, как они используют искусственный интеллект, какие данные они обрабатывают и для каких целей, а также должны быть готовы отвечать за свои действия перед обществом. Кроме того, необходимо учитывать мнение и интересы граждан при разработке и внедрении систем искусственного интеллекта в правоохранительные органы.

Таким образом, использование искусственного интеллекта в правоохранительной системе может быть полезным инструментом для оптимизации ее работы, но требует внимательного и осторожного подхода. Необходимо разработать правовые и этические принципы его использования в правоохранительной деятельности и обеспечить их соблюдение. Только тогда можно его использовать для улучшения работы правоохранительных органов и защиты прав и свобод граждан.

Список использованных источников:

1. Степанов Д.В. Интеллект, искусственный интеллект и право / Д.В. Степанов // Власть Закона. –2020. –№ 1 (41). – С. 97–103.

2. Канеев М.Ю., Махин С.А. Искусственный интеллект как современная отрасль психологического знания / М.Ю. Канеев, С.А. Махин // Психология и педагогика в Крыму: пути развития. – 2019. –№ 1. – С. 30–41.

3. Радченко Е.П., Монтлевич Т.А. Искусственный интеллект в правоохранительных органах / Е.П. Радченко, Т.А. Монтлевич // Научные труды ФКУ НИИ ФСИН России. – Москва, 2022. – С. 325–329.

4. Мезвришвили Н.К. Искусственный интеллект в сфере интеллектуальной собственности / Н.К. Мезвришвили // Труды по интеллектуальной собственности. – 2021. – Т. 38. –№ 3. – С. 99–103.

5. Емельянова Н.Ю., Рахмонбердиев Б.У. Искусственный интеллект в уголовном судопроизводстве / Н.Ю. Емельянова, Б.Б.У. Рахмонбердиев // Государственная служба и кадры. – 2022. –№ 5. – С. 188–190.

6. Себякин А.Г. Искусственный интеллект в криминалистике: система поддержки принятия решений / А.Г. Себякин //Baikal Research Journal. – 2019. – Т. 10. – № 4. – С. 21–30.

«Сот және құқық қорғау жүйесіндегі жасанды интеллект және үлкен деректер (BIG DATA): шындық және уақыт талабы» халықаралық ғылыми-тәжірибелік конференциясының қорытындысы бойынша ҰСЫНЫМДАР

«Сот және құқық қорғау жүйесіндегі жасанды интеллект және үлкен деректер (BIG DATA): шындық және уақыт талабы» Халықаралық ғылыми-тәжірибелік конференциясына қатысушылар Қазақстан Республикасының, Ресей Федерациясының және Өзбекстан Республикасының құқық қорғау және сот жүйесінің ғылыми және білім беру қауымдастығының сарапшылары мен өкілдерінің бірлескен қатысуы арқылы: *Қазақстан Республикасының Жоғарғы Соты, Ресей Федерациясы, Қазақстан Республикасының Бас прокуратурасы, Ресей Федерациясының Тергеу комитеті, Өзбекстан Республикасының Ғылым академиясы, Ресей Федерациясының Әділет министрлігі, Қазақстан Республикасының, Ресей Федерациясының және Өзбекстан Республикасының жоғары оқу орындары,* келесі тұжырымдар мен ұсыныстар әзірледі.

Жасанды интеллект – ол адам анықтаған мақсаттарда, деректерді талдау және онымен жасанды интеллект өзара әрекеттесетін қоршаған ортаға бейімделетін және әсер ететін анықталған заңдылықтар негізінде болжамдарды, ұсыныстарды немесе шешімдерді жасау арқылы шешілетін міндеттер бойынша адамның когнитивтік функцияларын имитациялауға мүмкіндік беретін технологиялық шешімдердің жиынтығы.

Бүгінгі таңда жасанды интеллект есептеу қуатының артуы, деректердің үлкен көлемінің жинақталуы және 5G сияқты желілердің дамуы есебінен өсіп келе жатқан стратегиялық технология екені даусыз.

2018 жылдан бастап көптеген елдер жасанды интеллектті дамытудың стратегияларын әзірлеп, бекітті. Халықаралық тәжірибені зерделеу көрсеткендей, қылмыстың қайталануын болжау, қалыптан тыс мінез-құлық детекторлары, сот үкімін шығаруды болжау жасанды интеллектті дамытудың тартымды бағыттарының бірі болып табылады.

Жасанды интеллект қылмыстық сот төрелігі саласына қатысты адамды ауыстыру ретінде қарастырылмауы керек. Бұл оның мүмкіндіктерін, қабілетін және адами әлеуетін арттыруға, болжау, тергеу тиімділігін, сот тәжірибесінің бірегейлігін және азаматтардың құқықтарын сапалы қорғауды қамтамасыз етуге көмектесетін қосымша құрал.

1. Қылмыстық сот төрелігі адамдардың өзара әрекеттесуімен жүзеге асырылатын қызмет және ол ең алдымен әлеуметтік технологияларды дамытады және осы қызметтің мақсаттарына жетуді қамтамасыз ететін осындай өзара әрекеттесу әдістерінің, құралдарының, тәсілдерінің белгілі бір жиынтығын қалыптастырады. Танымның ең

табысты әлеуметтік технологиялары процестік-құқықтық реттеуді алып, дәлелдеу құқығының нормаларына айналады.

Цифрлық технологиялардың пайда болуы және олардың қоғамдық қатынастар саласына толық енуі жалпы құқыққа және қылмыстық-процестік танымына, атап айтқанда, дәлелдеуге әсер етпей қоймайды.

Сандық тіл адамдардың еркін әлеуметтік қарым-қатынасына арналмаған. Ол адам мен машинаның өзара әрекеттесуі үшін жасалған және адам машинаға командаларды беру және оның реакциясын қабылдау үшін жасанды, формальды алгоритмдік нәрсені жасайды. Мұндай өзара әрекеттесудегі құқықтық мағыналарды ашу үшін аудармашы емес, *интерпретатор* қажет. Ол әрбір цифрлық командалық кодтың мәні мен мақсатын түсінуі керек; машинаның қандай реакция тудыратынын білу; «адам-машина-адам» өзара әрекеттесу процесін адам тілінде түсіндіре білу.

2. Компьютерлік (кибер) қылмыстар бойынша қылмыстық істер бойынша дәлелдемелерді түрлендіру қажет және бұлтартпас, бірақ ол адвокаттардың цифрлық технологиялар саласындағы мамандармен кәсіби өзара іс-қимылын және бірлескен зерттеулерін талап етеді.

Сот ісін жүргізуді технологияландырудың нәтижесі цифрлық сот өндірісіне көшу болады, яғни соттың, іске қатысушы тұлғалардың және процеске басқа да қатысушылардың, сондай-ақ цифрлық деректер шешуші фактор болып табылатын сот шешімдерін орындау органдарының қызметі процестік құқық нормаларымен реттеледі, талдау нәтижелерін өңдеу және пайдалану дәстүрлі сот ісін жүргізу нысандарымен салыстырғанда, оның тиімділігін айтарлықтай арттыруға мүмкіндік береді.

Бұл қызметтегі ең маңызды процестер мыналар:

1. сот ісін жүргізу мақсаттары үшін маңызды ақпаратты машинада оқылатын ақпаратқа алу және түрлендіру;
2. оның одан әрі жинақталуы,
3. алынған ақпаратты талдау және өңдеу;
4. ұсынылған шешімді қалыптастыру,
5. ақпаратты адам оқи алатын пішінге кері түрлендіру;
6. алынған нәтижелерді пайдалану.

3. Жасанды интеллектті қолдану процесінде ең маңыздысы пайдаланушыларды басқару принципі болып табылады, оған сәйкес судья-адам жасанды интеллекттің ұсынысын жоққа шығарып, іс бойынша өз шешімін қабылдай алу мүмкіндігі болуы керек, ал процеске қатысушылар тікелей адам сотына (адамдардан тұратын) шағымдануға және жасанды интеллектпен шығарылған шешімге қарсы шығуға қабілетті болуы керек.

Мамандар арасындағы даулардың көпшілігі адамға жаза тағайындау, яғни машинамен шешім қабылдау, жасалған әрекеттің себебін ескеру, жеңілдететін жағдайлардың болуы, соның ішінде кінәлінің эмоционалды жағдайына негізделген. Бірақ мұндай шешім қалай, қандай алгоритм негізінде қабылданатынын түсіну бірдей маңызды.

Адам оқитын шешім жобасы адамның түпкілікті бағалауы мен шешім қабылдауы үшін жасанды интеллект белгілі бір қорытынды жасауға мүмкіндік берген факторларға сілтеме жасауы керек.

Сот ісін жүргізуді технологияландыру бойынша жұмыс үлкен кадрлық, материалдық, уақытша және басқа ресурстарды қажет етеді, бірақ қазір заң қауымдастығы алға жылжитын жолға балама жоқ, және бұл қызмет неғұрлым ертерек және белсенді болса, нәтиже соғұрлым тиімді болады.

4. Қылмыстық экономикалық, әлеуметтік-саяси және басқа мақсаттарда қашықтықтан оқыту технологиялары арқылы қылмыс жасаудан бастап нейрондық желілер мен жасанды интеллект технологияларын қолдануға дейін ең жаңа жоғары технологиялық құралдар қолданылады.

Үлкен деректерді талдау және пайдалану бойынша құқық қорғау шаралары қазіргі уақытта анық жеткіліксіз. Интернеттегі ақпаратты мемлекеттік бақылау және оларды тергеу мақсатында, жалпы алғанда, сот ісін жүргізу үшін пайдалану әрекеттері дайындықсыз және анық шектелген.

Сот билігінің мүддесі үшін үлкен деректерді кеңінен қолдануды ұйымдастырудың бұл баяулауы келесі ұйымдастырушылық проблемалардың шиеленісуін тудырады:

- үлкен деректерді талдаудың қиындығы;
- қылмыстық құқық бұзушылықтардың дамуын дұрыс емес болжау;
- қылмыстың алдын алу мақсатында қылмыстық жағдайға мемлекеттің әрекет етуінің тиімді үлгілерінің жоқтығы және т.б.

Сот өндірісінде үлкен деректерді (Big Data) қалыптастыруға және пайдалануға ерекше назар аудару керек. Осыған байланысты ғылыми зерттеулер мен сандық технологияларға, соның ішінде жасанды интеллектке негізделген инновациялық құралдар мен әдістерді әзірлеу, оларды кейіннен ұйымдастырушылық-құқықтық реттей отырып, тәжірибеде Big Data өңдеу және пайдалану өзекті болып табылады.

Осы мақсатта келесі шаралар ұсынылады:

1. Үлкен деректерді (соның ішінде әмбебап геномдық тіркеу ел тұрғындарының деректер базасы) қалыптастыру мен пайдалануды реттейтін этикалық талаптар туралы ережелерді қоса алғанда, сот ісін жүргізудің өзекті қолданбалы мәселелерін шешуде үлкен деректерді

пайдалануды толығымен заңдастыру мақсатында Big Data пайдаланудың ұйымдық-құқықтық негіздерін әзірлеу.

2. Тергеушілерді, анықтаушыларды, сот сарапшыларын, сондай-ақ судьялардың біліктілігін арттыру жүйесінде ақпараттық оқытудың жаңа бөлімін – «Үлкен деректерді (Big Data) пайдаланудың сот-сараптамалық құралдары мен әдістері» атты кәсіби оқыту бағдарламаларын әзірлеу және енгізу.

3. NoSQL, MapReduce, Hadoop және нейрондық желілердің танымал бағдарламалық үлгілерін пайдалануды қоса, өздігінен білім алу қасиеттері бар когнитивті есептеулерге негізделген сараптамалық жүйелерді әзірлеу. Мұндай жұмыстарды жүзеге асыру үшін, әрине, белгілі бір қаржылық және адам ресурстары бөлінуі керек.

4. IBM, Fujitsu (Жапония) компаниясынан Summit класындағы суперкомпьютерлерді сатып алу (немесе өз өндірісі) арқылы үлкен деректерді пайдалану үшін логистика деңгейін көтеру.

5. Құқық қорғау органдарының, оның ішінде соттардың жүйесінде үлкен деректер (Big Data) мүмкіндіктерін пайдалану бойынша жоғары білікті бөлімшелер құру және олардың осындай дерекқорларға қол жеткізуінің техникалық мүмкіндігін қамтамасыз ету.

6. Инновациялық зерттеу әдістерін табысты енгізу үшін құқық қорғау органдары қызметкерлерінің кәсіби даярлық деңгейін көтеру.

7. Құқық қорғау органдарының сот өндірісінде (қылмыскерлер мен хабар-ошарсыз кеткен адамдарды халықаралық іздеуден басталып, ұйымдасқан киберқылмыспен күреске дейін) құқық қорғау органдарының тығыз ынтымақтастығы үшін тиісті халықаралық ұйымдық дизайнмен және нормативтік құқықтық консолидация (халықаралық конвенцияларды, келісімдерді және басқа да нормативтік құқықтық құжаттарды қабылдау).

Бұл үлкен деректерді (Big Data) пайдалануды ұйымдастырушылық-құқықтық реттеудегі кешенді тәсіл, ол сот ісін жүргізуде оларды пайдалану тиімділігін арттырады.

5. Дәстүрлі сот жүйесінде кездесетін бірқатар проблемалар бар *(сот төрелігіне қолжетімділіктің шектелуі, сот процесінің баяулығы, сот шешімдерінің сапасының біркелкі еместігі және адам факторының істің нәтижесіне ықтимал әсері).*

Жаңа технологияларды енгізу сот процесінің сапасы мен қолжетімділігіне оң әсер етумен қатар, заңның гуманизациялануы, киберқауіпсіздік проблемалары және заңнама мен сот жүйесінің инфрақұрылымын жаңа технологиялық шындықтарға бейімдеу қажеттілігі сияқты белгілі бір қиындықтарды тудыруы мүмкін.

Киберқауіпсіздікті қамтамасыз ету, құқықтық базаны дамыту, дәстүрлі сот жүйесін ақпараттық технологиялардың сын-қатерлеріне бейімдеу, барлық мүдделі тараптардың пікірлері мен тәжірибесін есепке

алу – сот жүйесіне жаңа технологияларды енгізу кезінде ескерілетін негізгі аспектілер.

Бұл бағыттағы маңызды қадам Цифрлық сот төрелігі кодексін қабылдау болып табылады, оның мақсаты ақпараттық технологиялар мен адам құқықтарын қорғауға негізделген жаңа ашық сот жүйесі үшін құқықтық негізді қамтамасыз ету болып табылады.

6. Сот және құқық қорғау қызметінде ЖИ қолданудың негізгі проблемалары көрсетілген.

Біріншіден, сот және құқық қорғау қызметінде қолданылатын жасанды интеллект жүйелеріне сенімді қамтамасыз ету. Өз кезегінде, сенімді қамтамасыз етумен байланысты мәселе ЖИ алгоритмдеріндегі ықтимал жүйелі қате болып табылады. ЖИ жүйелері оларға енгізілген деректер негізінде үйренеді. Жаттығуда пайдаланылған деректерде қиғаштық болса, ЖИ үлгісі де кемсітушілікке әкелетін қиғаштыққа ие болады.

Екіншіден, сот және құқық қорғау қызметінде ЖИ қолданудың ашықтығы мәселесі. ЖИ жүйелеріндегі шешім қабылдау процесі көбінесе бұлыңғыр, жүйенің белгілі бір шешімге қалай келгені туралы нақты түсініктеме жоқ. ЖИ алгоритмдері жиі «қара жәшіктер» ретінде қарастырылады, яғни алгоритмнің белгілі бір шешімге қалай келгенін түсіну қиын болуы мүмкін.

Үшіншіден, осы қызмет салаларында ЖИ пайдалану құпиялылықты бұзу сияқты этикалық мәселелерге әкелуі мүмкін. Жасанды интеллект үлгілерін құру үшін пайдаланылатын оқу деректері көбінесе жеке ақпаратты қамтиды. Жасанды интеллект жүйелері жеке тұлғалардан олардың келісімінсіз жеке деректерді де жинай алады.

Төртіншіден, ЖИ-ді сот және құқық қорғау қызметінде қолдану жұмыс орындарының қысқаруына, соның салдарынан әлеуметтік және экономикалық мәселелерге әкелуі мүмкін.

Осыны ескере отырып, әзірлеушілерге техникалық және психологиялық тұрғыдан сенуге болатын ЖИ жүйелерін жасауға шақырылады.

7. Сот төрелігінде жасанды интеллектті пайдалану белгілі бір тәуекелдерді тудырады: робот машинасы жинаған және өңдейтін дәлелдемелердің рұқсат етілгендігі қандай, мұндай шешімдер, үкімдер заңды күшке ие бола ма? Сондықтан оны жүзеге асыру үшін берік ғылыми-практикалық негіз қажет. Тәжірибешілерге инновацияларды қауіпсіз енгізу үшін көп жұмыс істеу керек. Мүмкін болатын қателер мен бұзушылықтарға жауап беру сценарийлері қажет. Заңдарды терең қайта қарау қажет. Жаңа құқық бұзушылықтар немесе квалификациялық белгілерді енгізу туралы ойлану керек.

8. Қылмыстық-процестік, сот-сараптама қызметі жаһандық цифрландыру жағдайында тез өзгеруде, Қазақстан сияқты Ресей де трансформация процестеріне белсенді қатысуда. Қазақстан Республикасының электрондық құжат айналымын жүргізу тәжірибесін және қылмыстық істерді «электрондық» форматта тергеп-тексеру мүмкіндігін зерделеу бұл салада назар аударуды қажет ететін елеулі жетістіктерді көрсетеді.

Жалпы инновациялар тұрғысынан алғанда, сот сараптамасы ғылымының қолданбалы сипатына байланысты жаһандық цифрландыру жағдайында қазіргі және болашақ тергеушілерді даярлау сапасын арттыру үшін жалпы және жеке инновациялық әдістер ұсынылады.

Жалпы инновациялық әдістерге мыналар жатады:

1) Оқу аудио және бейне өнімдерін, соның ішінде веб-сайттарда, әлеуметтік желілерде және мессенджерлерде пайдалану.

2) Сот сараптамасында геймификация технологияларын қолдану, компьютерлік ойындарды, мамандандырылған компьютерлік бағдарламалар мен мобильді қосымшаларды және басқа да білім беру электрондық ресурстарын әзірлеу. Бірақ одан әрі табысты даму заңгерлер мен IT-мамандарының ұжымдық дамуының нәтижесінде, сондай-ақ тиісті, негізінен бюджеттік қаржыландыру арқылы қамтамасыз етілуі мүмкін.

3) Қолданбалы зерттеулердің пәнаралық байланысы.

Цифрландыру жағдайында тергеушілерді оқытудың жеке инновациялық әдістеріне мыналар жатады:

1) Мақсатты әзірлеу (жоғарыда аталған жалпы әдістерге, «компьютерлік» немесе киберқылмыс деп аталатын қылмыстарды тергеудің заманауи криминалистикалық әдістеріне, сондай-ақ тиісті тактикаға, тактикалық операциялар мен комбинацияларға негізделген.

2) Компьютерлік сот сараптамасын тағайындау, тергеушінің ақпараттық технологиялар саласындағы сарапшылармен және мамандармен, жедел-іздестіру және жедел-техникалық бөлімшелердің тиісті қызметкерлерімен өзара іс-қимылы мәселелері практиканың өзекті мәселелері болып табылады.

Сонымен, криминалистика ғылым ретінде ғана емес, сонымен қатар қызықты, қолжетімді, қолданбалы ұсыныстардың, сондай-ақ ұқсас дидактикалық құралдардың жиынтығы ретінде үнемі дамуы керек.

9. Математикалық статистика және жасанды интеллект әдістерін қолдану әртүрлі дәрежелі саны бар 27 белгілерін қамтитын сериялық қылмыстардың сандық криминалистикалық моделін құруға, сондай-ақ олардың жүйесінің белгілері арасындағы тұрақты байланыстарды анықтауға мүмкіндік берді. Зерттелетін қылмыстардың заңдылықтары белгілерді таңдауды анықтады, оның негізінде анық емес қылмыстардың және оларға қатысы бар адамдардың қатарлы сипатын белгілеуге

болады. Мұндай белгілер ретінде қылмыс болған жердің географиялық координаттары, әрекеттің жасалған уақыты (алғашқы және соңғы), оқиға болған жердің түрі, әдісі мен құралдары, жәбірленушінің жасы әсер етті. Бұл белгілер дәлелді айнымалыларға айналады. Әзірленген бағдарламалық жасақтаманы әртүрлі сериялық қылмыс түрлерімен жұмыс істеу үшін пайдалануға болады.

Осылайша, жасанды интеллектті қолдану мүмкіндігі туралы гипотеза:

а) сериялы қылмыскердің іздеу портретін құру;

б) ашылмаған әрекеттердің қатарында бірізді сипаттағы және бір субъекті жасаған әрекеттерді анықтау (қылмыстың байланысын анықтау);

в) қылмыскерлердің деректер базасына енгізілген тұлғалардың ішінен ең ықтимал күдіктіні анықтау (сезіктіге басымдық беру).

Осыны негізге ала отырып, әртүрлі қылмыс түрлерін, соның ішінде сериялық қылмыстарды тергеуде модельдеуде жасанды интеллект мүмкіндіктерін зерттеуді жалғастырған жөн.

10. Киберқауіпсіздік қазіргі заманғы мемлекеттің егемендігінің маңызды құрамдас бөлігі болып табылады. Мемлекеттердің цифрлық технологияларға тәуелділігі мен осы технологияларды қолданумен байланысты қауіп-қатерлерге байланысты киберқауіпсіздіктің жоғары деңгейін қамтамасыз ету қажеттілікке айналады.

Тиісті инфрақұрылымды дамыту, мамандандырылған институттарды құру, заңнаманы жетілдіру және халықаралық ынтымақтастық тәуелсіз саясатты жүзеге асыруды қамтамасыз етеді, киберқауіптердің күшеюі жағдайында қоғамның тұрақтылығына кепілдік береді.

11. Цифрлық трансформация стратегиясы киберқауіпсіздіктің ақпараттық технологиялар негізін әзірлеуге және құруға арналған көпір болып табылады. Сонымен қатар қазіргі кезеңде мемлекеттік басқару жүйесіндегі ақпараттық-технологиялық база блогын одан әрі дамыту мен жетілдірудің жаңа жолдарын құру және іздестіру басым бағыт болып табылады.

Цифрлық трансформация саласындағы барлық концепцияларды біріктіретін ортақ ұмтылыс – олардың цифрлық кеңістікті, сауаттылықты, киберқауіпсіздікті, осы процесті ғылыми, әдістемелік және құқықтық қамтамасыз етуді нығайту идеясына шоғырлануы.

Осы тұрғыда цифрлық трансформация стратегиясын құрудың негізгі тәсілдері мен принциптері мыналар болуы керек:

- ғылыми көзқарас пен нақтылық, заманауи білімге, әдістер мен технологияларға сүйену;

- кәсіби көзқарас;

- шешім қабылдаудың уақтылылығы, мақсаттылығы, олардың әлеуметтік, құқықтық және басқа да салдарын болжау;

- іс-әрекеттің мақсаттылығы, шынайылығы және ұтымдылығы;

- цифрландыруды дамыту бағыттарының барлық құрамдас бөліктерінің бірлігі.

12. Қазіргі уақытта Интернетті, соның ішінде Darknet технологияларын пайдаланатын қылмыстардың өсуі байқалады. Оларды ашу және зерттеу бірқатар қиындықтармен байланысты, олардың ең маңыздыларының бірі:

- шартты түрде «анонимайзер» деп аталатын Интернетте ақпаратты криптографиялық түрлендіру алгоритмдері және әртүрлі деректер алмасу схемалары негізінде жұмыс істейтін арнайы бағдарламалық құралдарды қолдану есебінен із қалыптастыру механизмінің ерекшелігі. Осыған байланысты криминалистикалық айналымға байланыс желілері арқылы байланыс және (немесе) интернет-провайдерлерінің коммутациялық жабдығы арқылы қылмыскердің компьютерінен жәбірленушінің компьютеріне немесе кері тәртіпте (тергеу жағдайына байланысты) компьютерлік ақпараттың өтуі туралы уақыт бойынша дәйекті түрде орналастырылған және логикалық өзара байланысқан бірнеше жазбалардан тұратын Интернетте іздерді қалыптастыру жүйесі болып табылатын «электрондық із» терминін енгізу ұсынылады.

«Darknet» технологиясының өзін Интернет желісінде ақпаратты іздеу, жинау, сақтау, өңдеу, беру, тарату және қорғау процестері мен әдістері, сондай-ақ Интернет желісінде жасалатын іс-әрекеттердің анонимділігі мен құпиялылығын сақтау үшін қолданылатын мамандандырылған бағдарламалық жасақтаманы пайдалануға негізделген осындай процестер мен әдістерді жүзеге асыру әдістері ретінде анықтауға болады.

Криминалистикалық тұрғыдан оны келесі түрлерге жіктеуге болады:

1) іздеу жүйелері (Интернет браузерлері), мысалы, Tor (ағылшынша The Onion Router қысқартылған) және I2P (ағылшынша Invisible Internet Project, IIP, I2P - Invisible Internet Project-тен);

2) Whonix, Subgraph, Tails сияқты операциялық жүйелер;

3) Freenet сияқты деректердің бұлттық қоймалары.

13. Іс жүзінде барлық посткеңестік мемлекеттерде киберқауіпсіздіктің ұлттық жүйесін қалыптастырудың құқықтық негіздері қаланды, ол негізінен тұжырымдамалық сипаттағы бірқатар нормативтік құқықтық актілерді дайындау мен қабылдауда көрініс тапты. Сонымен қатар, мұндай құжаттар тиісті қоғамдық қатынастардың даму динамикасын және ерекшеліктерін ескере отырып түзетуге жатады.

Қызмет саласының ерекшеліктеріне сүйене отырып, киберқауіпсіздікті құқықтық реттеу тұрғысынан «ізашарлардың» бірі банк секторы болып табылады. Бұл ретте, банк секторындағы кибершабуылдарға қарсы іс-қимыл әдістемесін жетілдіру ақпараттық қауіпсіздік стандарттарының пакетін әзірлеуді көздейді, оның ішінде басқа талаптармен қатар:

- киберқауіпсіздікті басқару жүйелеріне;
- виртуализация технологияларын пайдалану кезінде киберқауіпсіздікті қамтамасыз ету;
- киберқауіптерді басқару;
- банк секторы субъектілерінің киберқауіпсіздігінің стандарттар талаптарына сәйкестігін бағалау;
- стандарттардың талаптарына сәйкес киберқауіпсіздікті қамтамасыз ету саласындағы қызметті құжаттамалық қамтамасыз ету бойынша;
- киберқауіптерді және киберинциденттерді басқару;
- мобильді бағдарламалық өнімдердің (мобильді қосымшалардың) киберқауіпсіздігін қамтамасыз ету.

14. Бүгінгі таңда жасанды интеллекттің адам құқықтарына екі жақты әсерін айту қажет: бір жағынан, қылмыстың алдын алу, қылмыстық қудалау және сот ісін жүргізуде үлкен мүмкіндіктер анықталады, екінші жағынан, жеке адам құқықтарының бұзылу қаупі нақты көрсетілген.

ЖИ пайдалы болғанымен, ықтимал тәуекелдер мен этикалық салдарларды білу және оның жеке құқықтары мен бостандықтарын құрметтейтін түрде қолданылуын қамтамасыз ету маңызды. Осылайша осы озық технологияны пайдалана отырып, оның ықтимал зиянын азайта аласыз.

Осы мақсатта негізгі адам құқықтарын құрметтеу саласында ЖИ қолданумен байланысты этикалық мәселелердің бірнеше ықтимал шешімдері ұсынылады:

- адамның негізгі құқықтарын сақтай отырып, жасанды интеллектті дұрыс пайдалануды белгілейтін этикалық стандарттар мен нұсқаулықтарды әзірлеу және белгілеу;
- әсіресе жеке өмірге қол сұғылмаушылық, кемсітпеушілік және ашықтық сияқты салаларда ЖИ пайдалану шеңберін белгілейтін нормативтік құқықтық базаны құру;
- ЖИ әзірлеушілері мен адам құқықтары жөніндегі сарапшылар арасындағы ынтымақтастыққа, олардың технологияларындағы ықтимал алалаушылықтарды, кемсітушілік нәтижелерді және басқа да этикалық проблемаларды анықтауға ықпал ету;
- ЖИ жүйелерінде қолданылатын деректер мен алгоритмдерге қатысты ашықтықты арттыру;

- азаматтардың жеке деректерін бақылау мүмкіндігін кеңейту және оларға осы деректердің қалай пайдаланылатыны туралы ақпарат беру;

- тәуелсіз үшінші тарап ұйымдарының адамның негізгі құқықтары сақталатындай етіп әзірленуін және пайдаланылуын қамтамасыз ету үшін ЖИ жүйелеріне тұрақты аудит жүргізу;

- ЖИ пайдаланатын компаниялардың қызметкерлерін этикалық пайдалану мәселелері бойынша олардың білім алуын және кәсіби даярлығын қамтамасыз ету.

15. Жасанды интеллект технологияларын қолдануды нақты құқықтық реттеу жоқ. Жасанды интеллект технологияларын құқық қолдану практикасында, оның ішінде судьялық практикада қолданудың шектері мен мүмкіндіктерін анықтау өзекті міндет болып табылады.

«Цифр» сәніне сүйене отырып, олар цифрлық сот төрелігі, цифрлық қылмыс, цифрлық полиция, кибер әділеттілік туралы айта бастады. Қазіргі уақытта осындай көптеген терминдер бар. Сонымен қатар, авторлардың әрқайсысы осы терминдермен әр түрлі мағынаны түсінеді, дегенмен әр сөздің өзіндік семантикалық жүктемесі бар. Бұл жасанды интеллектпен де болды.

Интеллект – тірі организмнің табиғаттан-адамнан берілген қасиеті. Яғни, жасанды интеллект туралы айтатын болсақ, адамның қасиеті белгілі бір техникалық құралға, механизмге, аппаратқа ауысады.

Жасанды интеллект - бұл бағдарламашылар адамның интеллектісі деп санайтын нәрсеге еліктеу. Яғни, олар интеллект туралы өз идеяларын жүзеге асырады және оны жасамайды. Мұны істеу мүмкін емес. Жасанды интеллект шын мәнінде жалпы қабылданған мағынада интеллект емес, тек оның имитациясы, жалғандығы.

Инженерлердің филологтармен және заңгерлермен тығыз ынтымақтастығы қажет.

16. ЖИ-мен байланысты қызмет субъектілері ЖИ жүйесінің өмірлік циклінде оларды қолданудың кемсітушілік тәсілдерінің (нәсіліне, жынысына, ұлтына, әлеуметтік тегіне, дініне, саяси немесе өзге де сенімдеріне, терісінің түсіне, жасына, тіліне, туу жағдайларына, дене кемістіктеріне және кез келген өзге де факторларға байланысты кемсітушілік тәсілдерінің көріністерін барынша азайту үшін барынша күш салуы тиіс).

Бұл үшін оның феноменологиялық нұсқасы қолайлы, ол адами құндылықтарды сенсорлық әрекеттердің көрінісі ретінде түсіндіреді. Феноменологиялық этикаға назар аудару жасанды интеллектке тәжірибе жасау, эмпатияны сезіну, жаман әрекеттерді жақсы нәрселерден ажырату қабілетін енгізілген мәліметтер жиынтығы негізінде емес, жалпы қабылданған мораль мен адамгершілік, адалдық пен гуманизм нормалары негізінде енгізуге мүмкіндік береді.

Осылайша ұйымдастырылған жасанды интеллект жүйесі адам қызметінің көптеген салаларында, соның ішінде құқық қорғау саласында да тиімді жұмыс істей алады.

Феноменологиялық этика принциптерін сақтамай, «күшті» жасанды интеллект адамзат өркениетіне айтарлықтай қауіп төндіреді. Күш-жігерді жасанды интеллектті басқарудың сенімді жүйелерін құруға бағыттау қажет. ЖИ даму қарқыны тәуекелдер мен қауіптерді түсіну қарқынынан әлдеқайда озық екенін есте ұстаған жөн.

17. Құқықтық қатынастар тараптардың тиісті құқықтық нормаларда белгіленген субъективті құқықтық құқықтары мен міндеттерінің болуымен сипатталады. Құқықтық қатынас әрқашан екі жақты байланыс болып табылады. Құқықтық қатынастардың мазмұны субъективті құқықтық құқықтар мен міндеттерді құрайды. Субъективті құқықтық құқық үш өкілеттіктен тұрады: өз іс-әрекеттеріне, басқа тараптан міндеттемені орындауды талап етуге, талап қоюға.

Жасанды интеллект тасымалдаушы аппаратының нейрондық бағдарламалық қамтамасыз етуі жеке тұлғаның немесе бағдарламашы тұлғалар тобының (бағдарламашылардың) шығармашылық қызметінің нәтижесі болып табылады. Олар субъективті құқықтық құқықтар мен міндеттердің иелері болып табылады.

Алайда, белгілі бір кезеңде бұл бағдарламалық жасақтаманың дамуы автордың (авторлардың) қатысуынсыз және әсерінсіз мүмкін болады. Яғни, құрылғының өзі болжау мүмкін емес жаңа ақпарат шығара алады. Сонымен қатар, жасанды интеллект жасалған техникалық құрал, аппарат, механизм субъективті құқықтық құқықтар мен міндеттердің тасымалдаушысы болып табылмайды, өйткені ол үшін қажетті қасиеттерге ие емес.

Құқық нормасы болмаған жағдайда құқықтық қатынас мүмкін емес. Сондықтан жасанды интеллект технологияларын қолдану процесін ретке келтіру мақсатында оны құқықтық қамтамасыз ету маңызды.

Жасанды интеллект технологияларын пайдаланудың бірыңғай тәсілдерін әзірлеу, оны құқық қолдану практикасына, оның ішінде сот төрелігіне енгізудің бағыттары мен нысандарын жүйелеу қажет.

Әрине, құқық қолдану практикасында туындайтын құқықтық қатынастардағы жасанды интеллекттің жағдайы нақты анықталуы керек. Оның мақсаты басқару функцияларын қамтамасыз ету, ретке келтіру, құқық қолданушының қызметін ұйымдастырушылық қамтамасыз ету болып көрінеді.

Бұл жағдайда құқықтық қатынастардың субъектісі тек құқық қолданушы-адам бола алады. Жасанды интеллект бар Механизм-бұл тек көмекші, жұмысты оңтайландыруға, жеделдетуге, жетілдіруге мүмкіндік беретін техникалық құрал. Сондықтан оны пайдалану шегі қажет.

Механизмнің сипаты үшін заңды жауапкершілік – құқық қолданушының тағдыры. Оның міндеті-рұқсат етілмегенге жүгінбеу, құқықтық қатынастарға қатысушылардың құқықтарын қорғауды қамтамасыз ету мүддесінде процесті бақылау.

18. Жалпы қоғам үшін қауіпсіздік пен пайдалылық кепілдіктері үшін реттеудің белгілі бір түрі қажет. Жасанды интеллекттің халықаралық-құқықтық реттелуі қарқынды дамып келе жатқан ЖИ сипатына сәйкес келетін икемді болуы керек. Жасанды интеллект дамып, жаңа технологиялар мен қосымшалар пайда бола бастаған кезде, нормативтік құқықтық база осы өзгерістерге бейімделіп, адам құқықтары саласындағы этикалық стандарттар мен стандарттарға сәйкес жасанды интеллекттің дамуы мен қолданылуын қамтамасыз етуі керек.

19. Сот жүйесінде және сот төрелігін жүзеге асыруда жасанды интеллектті қолданудың бірнеше халықаралық-құқықтық аспектілері бар, оларды ескеру қажет:

- сот төрелігін жүзеге асыруда қолданылатын кез-келген жасанды интеллект жүйесі бұл адам құқықтарын бұзбауы керек. ЖИ жүйелерін оқыту үшін пайдаланылатын деректердегі кез келген қателер анықталып, жойылуы керек және олардың қоғамның әртүрлі әлеуметтік топтарына әсері қатаң ескерілуі керек.
- ашықтық пен есеп беру дегеніміз, осы контексттерде қолданылатын кез-келген ЖИ жүйелерінің шешім қабылдау процестері тексеруге ашық болуы керек, ал оларды әзірлеуге және орналастыруға жауапты адамдар оларды қолданудың кез-келген зияны үшін жауап беруі керек.
- құпиялылық және деректерді қорғау осы контексттерде ЖИ жүйелері пайдаланатын кез келген деректерді қолданыстағы деректерді қорғау заңдарына сәйкес жинау және пайдалану керек дегенді білдіреді.
- сот жүйесі мен сот төрелігінде ЖИ қолдану автономия, игілік, зиян келтірмеу және әділеттілік принциптерін қоса алғанда, этикалық ойларға сәйкес келуі керек.

Бұл ретте, озық әлемдік тәжірибені пайдалана отырып, IT-сервистер арқылы сот төрелігіне ыңғайлы және кедергісіз қол жеткізуді қамтамасыз ету; деректерді өңдеу процестерін автоматтандыру арқылы сот ісін жүргізуді неғұрлым ашық және үнемді ете отырып, оңайлату және жеделдету; сот қорғауының сапасын арттыруға және күш органдарының құқық қорғау әлеуетін күшейтуге бағытталған цифрлық құралдарды енгізуді жалғастыру қажет.

Жасанды интеллект технологиясы қарқынды дамып келеді, бұл уақыт өте келе өзекті және тиімді болып қалатын ережелер мен стандарттарды әзірлеуді қиындатуы мүмкін. Осы міндеттер мен мәселелерді шешу әр түрлі елдердің саясаткерлері, заңгерлері мен

техникалық сарапшылары арасындағы ынтымақтастық пен ынтымақтастықты қажет етеді. Жасанды интеллект қарқынды дамып келе жатқандықтан, оны әзірлеу мен енгізуге байланысты құқықтық және этикалық мәселелерді шешу үшін мемлекеттер мен халықаралық ұйымдардың халықаралық ынтымақтастығы мен өзара іс-қимылына қажеттілік артып келеді.

20. Әлемнің көптеген елдерінде, әсіресе ақпараттық және телекоммуникациялық технологияларды қолданатын қылмыстар саласында өте күрделі қылмыстық жағдай байқалады. Бұл құқық қорғау органдары тарапынан, оның ішінде сот ісін жүргізуді ғылыми-техникалық қамтамасыз ету деңгейін арттыру жолымен елеулі оң іс-қимылдарды талап етеді.

Қазіргі кезеңде сот ісін жүргізу сапасын арттыру үшін сот сараптамаларының перспективалы инновациялық бағыттарын дамыту арқылы сот-сараптама қызметінің тиімділігін арттыру қажет.

Перспективалық бағыттар деп тану керек:

- ескі биологиялық үлгілердегі ДНҚ-ның қысқа бөліктерін анықтауға мүмкіндік беретін әрбір «снип» - тегі барлық төрт нуклеотидті бірден екілік форматта цифрландырудың түпнұсқа әдісі». Мұндай әдістерді қолдану кезінде максималды цифрландыруға қол жеткізіледі: снип көмегімен жеке тұлғаны ДНҚ-идентификациялау кезінде ақпарат көлемі бір адамға бір килобайттан аспайды (салыстыру үшін: қазіргі уақытта қолданылатын STR-локустардың көмегімен – 200 килобайттан астам)»;

- жазбаша белгілерді кодтаудың бағдарламалық қамтамасыз етуімен математикалық модельдеу әдістерін сот қолжазбалық сараптамасына енгізу;

- бейнебақылау камераларының көмегімен цифрлық тасымалдағышта түсірілген адамның динамикалық белгілері (мысалы, жүрісі) бойынша жеке басын сәйкестендіру - соттық бейнепортреттік сараптама;

- полиграфты қолдану арқылы психофизиологиялық сараптама. Сот сараптамасының осы түрінің ғылыми-негізделген әдістемесін кейіннен сертификаттай отырып, елеулі валидация жүргізу қажет.

Жасанды интеллектті қоса алғанда, инновациялық технологияларды сот ісін жүргізуге енгізу перспективалары олармен танысу үшін ғылыми-практикалық форумдарды: съездерді, симпозиумдарды, конференцияларды, семинарларды және сот-сараптама қызметі мәселелері жөніндегі басқа да іс-шараларды ұйымдастыру және жүйелі өткізу жолымен, шеберлік сыныптарын өткізу үшін жетекші тәжірибеші ғалым-сарапшыларды шақыра отырып, әлдеқайда жылдам іске асырылатын болады.

21. Блокчейн-технологияларды (смарт-келісімшарттар) қолдана отырып жасалған мәмілелерді құқықтық реттеу мәселелері электрондық мәмілелерден айырмашылығы қолданыстағы заңнама нормаларымен реттелмейді.

Олардың презентациясының нақты құрылымы, мәміле шарттарын жазу кезінде компьютерлік кодты қолдану шарттардың нақты түрін реттейтін заңнаманың жекелеген нормаларын қабылдауды талап етеді.

Қазақстан Республикасы Азаматтық кодексінің Ерекше бөлігінің дербес тарауын көздеп, жалпы бөлімнің жекелеген нормаларына өзгерістер мен толықтырулар енгізу қажет болуы мүмкін.

Егер тараптардың бірі мәселені мәжбүрлеп орындаудың және шартты бұзудың ішкі тетігімен реттеу нәтижесіне қанағаттанбаған жағдайда, жасалған смарт-келісімшарттар бойынша дауларды сотта қараудың рәсімі мен тәртібін айқындау талап етіледі.

22. «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Қазақстан Республикасы Заңының 1-бабының 12) тармақшасында қамтылған электрондық құжат ұғымын түзету қажет.

Қолданыстағы анықтама тар және компьютерлік код арқылы жасалған құжаттарды қамтымайды, өйткені олар тек электрондық цифрлық қолтаңба арқылы қол қойылған электрондық-цифрлық нысандағы құжаттарды білдіреді.

Заңнамаға тиісті өзгерістер мен толықтырулар енгізу блокчейн-технологияларды қолдана отырып смарт-келісімшарттар жасасу саласындағы құқықтық қатынастарды неғұрлым толық реттеуге, сондай-ақ осы құқықтық қатынастарға тартылған адамдардың құқықтарын қорғауға ықпал ететін болады.

РЕКОМЕНДАЦИИ
по результатам работы Международной научно-практической конференции: «Искусственный интеллект и большие данные (BIG DATA) в судебной и правоохранительной системе: реалии и требование времени»

Участники Международной научно-практической конференции: **«Искусственный интеллект и большие данные (BIG DATA) в судебной и правоохранительной системе: реалии и требование времени»,** посредством совместного участия экспертов научно-образовательного сообщества и представителей правоохранительной и судебной системы Республики Казахстан, Российской Федерации и Республики Узбекистан: *Верховного Суда Республики Казахстан, Российской Федерации, Генеральной прокуратуры Республики Казахстан, Следственного комитета Российской Федерации, Академии наук Республики Узбекистан, Министерства юстиции Российской Федерации, высших учебных заведений Республики Казахстан, Российской Федерации и Республики Узбекистан,* пришли к следующим выводам и рекомендациям.

Искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека, для целей, определенных человеком, по задачам, которые решаются путем генерации прогнозов, рекомендаций или решений на основе анализа данных и выявленных закономерностей, адаптируемых к среде и влияющих на среду, с которой искусственный интеллект взаимодействует.

На сегодня нет никаких сомнений, что искусственный интеллект – это стратегическая технология, которая растет благодаря увеличению вычислительных мощностей, накоплению большого массива данных и развитию сетей, таких как 5G.

С 2018 года большинством стран разработаны и утверждены стратегии развития искусственного интеллекта. Изучение международного опыта показывает, что прогнозирование рецидива правонарушений, детекторы аномального поведения, прогнозирование судебного решения входит в число привлекательных сфер для развития искусственного интеллекта

Искусственный интеллект не должен рассматриваться применительно к сфере уголовного судопроизводства как замена человека. Это лишь дополнительный инструмент повышения его возможностей, способностей и человеческого потенциала, помощи для обеспечения эффективности прогнозирования, расследования, единообразия судебной практики и качественной защиты прав граждан.

1. Уголовное судопроизводство — это деятельность, осуществляемая при взаимодействии людей, и, она, прежде всего, вырабатывает *социальные технологии* и формирует определенный набор методов, средств, приемов такого взаимодействия, обеспечивая достижение целей данной деятельности. Наиболее успешные социальные технологии познания получают процессуально-правовое регулирование и становятся нормами доказательственного права.

Появление *цифровых технологий* и их тотальное проникновение в сферу социальных отношений не может не затронуть право в целом и уголовно-процессуальное познание, и доказывание, в частности.

Цифровой язык не создан для свободного социального взаимодействия людей. Он создан для взаимодействия «человек-машина» и человек создает нечто искусственное, формально алгоритмичное для передачи команд машине и получения ее реакции. Чтобы выявить правовые смыслы в таком взаимодействии необходим не переводчик, а *интерпретатор.* Он должен понимать смысл и назначение каждой цифровой команды-кода; знать, какую реакцию машины это порождает; уметь объяснить человеческим языком весь процесс взаимодействия «человек-машина-человек».

2. Трансформация доказывания по уголовным делам о компьютерных (кибер) преступлениях необходима и неизбежна, однако она требует профессионального взаимодействия и совместных исследований юристов со специалистами в области цифровых технологий.

Результатом технологизации судопроизводства станет переход к цифровому судопроизводству, т.е. урегулированному нормами процессуального права деятельности суда, участвующих в деле лиц и других участников процесса, а также органов исполнения судебных решений по разрешению юридических дел, в которой ключевым фактором являются данные в цифровом виде, обработка и использование результатов анализа которых по сравнению с традиционными формами судопроизводства позволяют существенно повысить его эффективность.

Наиболее важными в этой деятельности представляются следующие процессы:

1. получение и трансформация релевантной для целей судопроизводства информации в машиночитаемую,
2. дальнейшее ее накопление,
3. анализ и обработка полученной информации,
4. формирование предлагаемого решения,
5. обратная трансформация информации в человекочитаемый вид,
6. использование полученных результатов.

3. Наиболее значимым в процессе применения искусственного интеллекта является принцип контроля пользователя, в соответствии с которым, судья - человек должен иметь возможность опровергнуть предложение искусственного интеллекта и принять собственное решение по делу, а участники процесса должны иметь возможность прямого обращения к человеческому суду (*состоящего из людей)* и оспорить решение, принятое искусственным интеллектом.

Большинство споров среди специалистов ведется по поводу назначения наказания человеку, т.е. по сути принятия решения машиной, учету мотива совершенного поступка, наличие смягчающих обстоятельств, в т.ч. и основанных на эмоциональном состоянии виновного. Но не менее важно понимать, как, на основе какого алгоритма, принимается такое решение.

Человекочитаемый проект решения должен содержать ссылку на те факторы, которые позволили ИИ сделать те или иные выводы для окончательной оценки и принятия решения человеком.

Работа по технологизации судопроизводства потребует больших кадровых, материальных, временных и иных ресурсов, но альтернативы пути, по которому продвигается сейчас юридическое сообщество нет, и чем раньше и активней будет осуществляется эта деятельность, тем эффективней будет результат.

4. В преступных экономических, социально-политических и иных целях используются новейшие высокотехнологичные средства: начиная от совершения преступлений с помощью дистанционных технологий до использования технологий нейронных сетей и искусственного интеллекта.

Меры правоохранительных органов по анализу и использованию Big Data в настоящее время явно недостаточны. Предпринимаемые попытки государственного контроля над информацией в сетях Интернет и их использования в целях расследования и, в целом, для судопроизводства являются неподготовленными и явно ограниченными.

Подобное замедление организации широкого использованием больших данных в интересах судопроизводства создает усугубление следующих организационных проблем:

- затруднение анализа больших данных;
- неточное прогнозирование развития преступных правонарушений;
- отсутствие эффективных моделей государственного реагирования на криминогенную ситуацию в целях предупреждения преступлений и т.д.

Особое внимание должно быть уделено вопросам формирования и использования больших данных (Big Data) в судопроизводстве. В этой связи актуальными являются научные исследования и разработки

инновационных средств и методов на базе цифровых технологий, включая искусственный интеллект, по обработке и использованию Big Data в практической деятельности, с их последующей организационно-правовой регламентацией.

Для этого предлагаются следующие меры:

5. Разработать организационно-правовые основы использования Big Data в целях полной легитимизации применения больших данных в деле решения актуальных прикладных задач судопроизводства, включив в них положения по этическим требованиям, которые регламентируют формирование и использование больших данных (в том числе, базы данных всеобщей геномной регистрации населения страны).

6. Разработать и включить в программы профессиональной подготовки следователей, оперуполномоченных, судебных экспертов, а также в системе повышения квалификации судей нового раздела информационной подготовки – «Криминалистические средства и методы использования больших данных (Big Data)».

7. Разработать экспертные системы, базирующиеся на когнитивных вычислениях, имеющих свойства самообучения, в том числе с использованием известных образцов программного обеспечения NoSQL, MapReduce, Hadoop и нейросетей. Для проведения такой работы, конечно же, должны выделяться определенные денежные и кадровые ресурсы.

8. Поднять уровень материально-технического обеспечения использования больших данных за счет приобретения (или собственного производства) суперкомпьютеров класса Summit от IBM, Fujitsu (Япония).

5. Создать в системе правоохранительных органов, включая суды, высококвалифицированные подразделения по использованию возможностей больших данных (Big Data) и обеспечить техническую возможность их доступа к таким базам данных.

6. Повысить уровень профессиональной подготовки сотрудников правоохранительных органов для успешного внедрения инновационных методов исследования.

7. Объединить усилия государств по тесному взаимодействию правоохранительных органов в деле использования больших данных в судопроизводстве (начиная с международного розыска преступников и без вести пропавших лиц и заканчивая борьбой с организованной киберпреступностью) с соответствующим международным организационным оформлением и нормативно-правовым закреплением (принятием международных Конвенций, соглашений и других нормативных правовых документов).

Именно комплексный подход в организационно-правовой регламентации использования больших данных (Big Data) позволит повысить эффективность их применения в судопроизводстве.

5. Существует ряд проблем, с которыми сталкивается традиционная судебная система *(ограниченный доступ к правосудию, медленность судебного процесса, неоднородность качества судебных решений и возможное воздействие человеческого фактора на исход дела).*

Внедрение новых технологий может наряду с положительным влиянием на качество и доступность судебного процесса, породить определенные вызовы, такие как дегуманизация права, проблемы кибербезопасности и необходимость адаптации законодательства и инфраструктуры судебной системы к новым технологическим реалиям.

Обеспечение кибербезопасности, разработка правовых рамок, адаптация традиционной судебной системы к вызовам информационных технологий и учет мнений и опыта всех заинтересованных сторон – ключевые аспекты, которые следует учитывать при внедрении новых технологий в судебную систему.

Важным шагом в этом направлении является Принятие Кодекса цифрового правосудия, цель которого - обеспечение правовых рамок для новой прозрачной судебной системы, основанной на информационных технологиях и защите прав человека.

6. Выделены основные проблемы использования ИИ в судебной и правоохранительной деятельности.

Во-первых, обеспечение доверия к системам искусственного интеллекта, применяемым в судебной и правоохранительной деятельности. В свою очередь, проблемой, связанной с обеспечением доверия, является потенциальная систематическая ошибка в алгоритмах ИИ. Системы ИИ обучаются на основе вводимых в них данных. Если данные, используемые при обучении, содержат систематическую ошибку, модель ИИ также будет иметь систематическую ошибку, что приведет к дискриминационным результатам.

Во-вторых, вопрос прозрачности использования ИИ в судебной и правоохранительной деятельности. Процесс принятия решений в системах ИИ часто непрозрачен, без четкого объяснения того, как система пришла к тому или иному решению. Алгоритмы ИИ часто рассматриваются как «черные ящики», а это означает, что может быть трудно, понять, как алгоритм пришел к конкретному решению.

В-третьих, использование ИИ в этих сферах деятельности может привести к этическим проблемам, таким как нарушение конфиденциальности. Данные обучения, используемые для создания моделей ИИ, часто содержат личную информацию. Системы

искусственного интеллекта также могут собирать личные данные отдельных лиц без их согласия.

В-четвертых, применение ИИ в судебной и правоохранительной деятельности может привести к сокращению рабочих мест, и, в результате к социальным и экономическим проблемам.

С учетом этого разработчикам рекомендуется создавать системы ИИ, которым можно доверять в техническом и психологическом плане.

7. Использование искусственного интеллекта в правосудии несёт в себе определенные риски: какова допустимость доказательств, собранных и обработанных робот-машиной, будут ли иметь юридическую силу такие постановления, приговоры? Поэтому, его внедрение требует прочную научно-практическую основу. Ученым-практикам предстоит большая работа по безопасному внедрению новшеств. Нужны сценарии реагирования на возможные ошибки и нарушения. Требуется глубокая ревизия законов. Необходимо задуматься о введении новых составов правонарушений или квалифицирующих признаков.

8. Уголовно-процессуальная, криминалистическая деятельность стремительно меняются в условиях глобальной цифровизации, Россия, как и Казахстан, активно вовлечены в трансформационные процессы. Изучение опыта Республики Казахстан ведения электронного документооборота и возможности расследования уголовных дел в «электронном» формате указывает на значимые успехи в этой области, заслуживающие пристального внимания.

С точки зрения общих инноваций в силу прикладного характера науки криминалистика, предложены общие и частные инновационные методы повышения качества обучения действующих и будущих следователей в условиях глобальной цифровизации.

К числу общих инновационных методов следует отнести:

1) Использование образовательной аудио и видео-продукции, в том числе, на сайтах, в социальных сетях и мессенджерах.

2) Использование технологий геймификации в криминалистике, разработка компьютерных игр, специализированных компьютерных программ и мобильных приложений, иных обучающих электронных ресурсов. Но дальнейшие успешные разработки могут быть обеспечены только в результате коллективных разработок юристов и IT-специалистов, а также при условии надлежащего, в основном бюджетного финансирования.

3) Междисциплинарность прикладных исследований.

К числу частных инновационных методов обучения следователей в условиях цифровизации следует отнести:

1) Целенаправленную разработку (на основе вышеизложенных общих методов, современных криминалистических методик расследования так называемых «компьютерных» или кибер-преступлений, а также соответствующих тактических приемов, тактических операций и комбинаций.

2) Вопросы назначения компьютерных судебных экспертиз, взаимодействия следователя с экспертами и специалистами в области информационных технологий, соответствующими сотрудниками оперативно-розыскных и оперативно-технических подразделений – насущные проблемы практики.

Таким образом, криминалистика должна постоянно развиваться не только как наука, но и как совокупность интересных, доступно изложенных, прикладных рекомендаций, а также аналогичных дидактических средств.

9. Применение методов математической статистики и искусственного интеллекта позволило построить цифровую криминалистическую модель серийных преступлений, содержащую 27 признаков с различным числом градаций, а также выявить закономерные связи между признаками их системы. Закономерности изученных преступлений детерминировали выбор признаков, на основе которых возможно устанавливать серийный характер неочевидных преступлений и причастных к ним лиц. В качестве таких признаков выступили географические координаты места преступления, время совершения деяния (начальное и конечное), вид места преступления, способ и орудия, возраст потерпевшего. Эти признаки преобразованы в доказательственные переменные. Разработанное программное обеспечение может применяться для работы с различными видами серийных преступлений.

Таким образом, подтверждена гипотеза о возможности использования искусственного интеллекта для:

а) построения поискового портрета серийного преступника;

б) выявления в массиве нераскрытых деяний тех, которые носят серийный характер и совершены одним и тем же субъектом (выявление связи преступлений);

в) установления наиболее вероятного подозреваемого из числа лиц, учтённых в базе данных о преступниках (приоритезация подозреваемого).

Исходя из этого, целесообразно продолжать исследования возможностей искусственного интеллекта в моделировании при расследовании различных видов преступлений, в том числе серийного характера.

10. Кибербезопасность является важной составляющей суверенитета современного государства. В условиях зависимости государств от цифровых технологий и угроз, связанных с использованием этих технологий, обеспечение высокого уровня кибербезопасности становится необходимостью.

Развитие соответствующей инфраструктуры, создание специализированных учреждений, совершенствование законодательства и международное сотрудничество позволят обеспечить проведение независимой политики, гарантировать устойчивость общества в контексте усиливающихся киберугроз.

11. Стратегия цифровой трансформации является плацдармом для развития и построения информационно-технологической основы в деле обеспечения кибербезопасности. При этом создание и поиск новых путей дальнейшего развития и совершенствования блока информационно-технологической основы в системе государственного управления на современном этапе является приоритетным направлением.

Общим устремлением, объединяющим все концепции в деле цифровой трансформации, является их ориентация на идею укрепления цифрового пространства, грамотности, кибербезопасности, научного, методического и правового сопровождения данного процесса.

В данном контексте, основными подходами и принципами построения стратегии цифровой трансформации должны выступать:

- научный подход и конкретность, опора на современные знания, методики и технологии;
- профессиональный подход;
- своевременность, целесообразность принятия решений, прогнозирование их социальных, правовых и других последствий;
- целенаправленность, реальность и рациональность действий;
- единство всех составляющих направлений развития цифровизации.

12. В настоящее время наблюдается колоссальное увеличение преступлений, с использованием сети Интернет, в том числе технологий «Даркнет». Их раскрытие и расследование сопряжено с рядом трудностей, из которых одним из наиболее значимых является:

- специфичность механизма следообразования, обусловленного применением специального программного обеспечения, работающего на основе алгоритмов криптографического преобразования информации и разных схем обмена данными в сети Интернет, условно называемых «анонимайзерами».

В этой связи предлагается ввести в криминалистический оборот термин «дорожка электронных следов», которая представляет собой

систему образования следов в сети Интернет, состоящую из нескольких последовательно расположенных по времени и логически взаимосвязанных записей о прохождении компьютерной информации по линиям связи через коммутационное оборудование оператора(-ов) связи и(или) провайдеров услуг Интернет от компьютера преступника до компьютера потерпевшего или в обратном порядке (в зависимости от следственной ситуации).

Саму же технологию «Даркнет» можно определить как процессы и методы поиска, сбора, хранения, обработки, предоставления, распространения и защиты информации в сети Интернет, а также способы осуществления таких процессов и методов, основанные на использовании специализированного программного обеспечения, применяемого для сохранения анонимности и приватности действий, совершаемых в сети Интернет.

С криминалистических позиций представляется возможным классифицировать ее на следующие виды:

1) поисковые системы (интернет-браузеры), например, такие как Tor (сокр. от англ. The Onion Router) и I2P (от англ. Invisible Internet Project, IIP, I2P – проект «Невидимый интернет»);

2) операционные системы типа Whonix, Subgraph, Tails;

3) облачные хранилища данных, например Freenet.

13. Практически во всех постсоветских государствах заложены правовые основы формирования национальной системы обеспечения кибербезопасности, что выразилось главным образом в подготовке и принятии ряда нормативных правовых актов концептуального характера. Кроме того, такие документы подвергаются корректировке с учетом динамики развития и специфики соответствующих общественных отношений.

Исходя из специфики сферы деятельности, одним из «пионеров» в части правового регулирования обеспечения кибербезопасности становится банковская сфера.

При этом, совершенствование методологии противодействия кибератакам в банковской сфере предполагает разработку пакета стандартов информационной безопасности, включающего, помимо прочего, требования:

- к системам управления кибербезопасностью;
- по обеспечению кибербезопасности при использовании технологий виртуализации;
- по управлению киберриском;
- по оценке соответствия кибербезопасности субъектов банковской сферы требованиям стандартов;

- по документационному обеспечению деятельности в области обеспечения кибербезопасности в соответствии с требованиями стандартов;

- управлению киберугрозами и киберинцидентами;

- по обеспечению кибербезопасности мобильных программных продуктов (мобильных приложений).

14. На сегодняшний день необходимо констатировать двоякое влияние ИИ на права человека: с одной стороны, определяются большие возможности в предупреждении преступности, уголовном преследовании и судебном рассмотрении, с другой стороны, четко обозначены угрозы нарушения отдельных прав человека.

При всей полезности ИИ, важно учитывать потенциальные риски и этические последствия, а также обеспечивать его использование таким образом, чтобы уважать права и свободы личности. Таким образом, можно использовать преимущества этой прогрессивной технологии, сводя к минимуму ее потенциальный вред.

В этих целях, предлагается несколько возможных вариантов решения этических проблем, связанных с использованием ИИ в области соблюдения основных прав человека:

- разработка и установление этических стандартов и руководящих принципов, предписывающих надлежащее использование ИИ с соблюдением основных прав человека;

- создание нормативной правовой базы, устанавливающей рамки использования ИИ, особенно в таких областях, как неприкосновенность частной жизни, недискриминация и прозрачность;

- способствование сотрудничеству между разработчиками ИИ и экспертами по правам человека, для выявления потенциальных предубеждений, дискриминационных результатов и других этических проблем в их технологиях;

- повышение прозрачности в отношении данных и алгоритмов, используемых в системах ИИ;

- расширение возможности граждан по контролю над своими личными данными и предоставление им информации о том, как используются эти данные;

- проведение регулярных аудитов систем ИИ независимыми сторонними организациями, чтобы гарантировать, что они разработаны и используются таким образом, чтобы соблюдались основные права человека;

- обеспечение образования и профессиональной подготовки сотрудников компаний, использующих ИИ, по вопросам их этичного использования.

15. Нет четкого правового регулирования применения технологий искусственного интеллекта. Насущной задачей является определение пределов и возможностей использования технологий искусственного интеллекта в правоприменительной практике, в том числе судейской.

Следуя моде на «цифру», стали говорить о цифровом правосудии, цифровой преступности, цифровом полицейском, киберправосудии. И подобных терминов в настоящее время существует великое множество. При этом каждый из авторов понимает под этими терминами нечто свое, хотя каждое слово имеет свою смысловую нагрузку. Это же произошло с искусственным интеллектом.

Интеллект - свойство живого организма, данное ему от природы – человека. То есть, говоря об искусственном интеллекте, свойство человека переносится на некое техническое средство, механизм, аппарат.

Искусственный интеллект-это имитация того, что программисты представляют себе как человеческий интеллект. То есть они реализуют свои представления об интеллекте, а не создают его. Это сделать и невозможно. Искусственный интеллект на самом деле вовсе не интеллект в общепринятом смысле, а лишь его имитация, подделка

Необходимо более тесное сотрудничество инженеров с филологами и юристами.

16. Субъекты, связанной с ИИ деятельности должны прилагать максимум усилий, чтобы минимизировать проявления в жизненном цикле системы ИИ дискриминационных способов их применения (дискриминационных по расовой принадлежности, гендерной принадлежности, национальности, социальному происхождению, вероисповеданию, политическим или иным убеждениям, цвету кожи, возрасту, языку, условиям рождения, физическим недостаткам и любым иным факторам).

Для этого более подходит её феноменологический вариант, который трактует человеческие ценности как результат проявления чувственных актов. Ориентация на феноменологическую этику позволит внедрить в искусственный разум способность переживать, испытывать эмпатию, отличать плохие поступки от хороших не на основе заложенного набора данных, а на основе общепринятых норм морали и нравственности, честности и гуманизма.

Организованная таким образом система ИИ будет способна эффективно функционировать во многих сферах человеческой деятельности, в том числе и в правоохранительной сфере.

Без поддержания принципов феноменологической этики «сильный» искусственный интеллект представляет существенную опасность для человеческой цивилизации. Необходимо сосредоточить усилия на создании надежных систем управления искусственным

интеллектом. Следует учитывать, что темпы развития ИИ значительно опережают темпы осмысления рисков и угроз.

17. Для правоотношения характерным является наличие у сторон субъективных юридических прав и обязанностей, которые устанавливаются соответствующими правовыми нормами. Правоотношение всегда двусторонняя связь. Содержание правоотношения составляют субъективные юридические права и обязанности. Субъективное юридическое право складывается из трех правомочий: на собственные действия, на требование от другой стороны исполнения обязанности, на притязание.

Нейросетевое программное обеспечение аппарата-носителя искусственного интеллекта является результатом творческой деятельности физического лица или группы лиц – программиста (программистов). Именно они и являются носителями субъективных юридических прав и обязанностей.

Однако на определенном этапе развитие этого программного обеспечения возможно и без участия и влияния автора (авторов). То есть сам аппарат может производить новую информацию, причем непредсказуемо. При этом техническое средство, аппарат, механизм, в котором заключен искусственный интеллект, не является носителем субъективных юридических прав и обязанностей, поскольку не обладает для этого необходимыми качествами.

Правоотношение при отсутствии нормы права невозможно. Поэтому в целях упорядочения процесса применения технологий искусственного интеллекта, важно его правовое обеспечение.

Необходимо выработать единые подходы к использованию технологий искусственного интеллекта, систематизировать направления и формы его внедрения в правоприменительную практику, в том числе правосудие.

Безусловно, четко должно быть определено положение искусственного интеллекта в правоотношении, возникающем в правоприменительной практике. Представляется, что его назначение состоит в обеспечении, упорядочении управленческих функций, организационном обеспечении деятельности правоприменителя.

При этом субъектом правоотношения может быть только правоприменитель – человек. Механизм, содержащий в себе искусственный интеллект, всего лишь помощник, техническое средство, позволяющее оптимизировать, ускорить, усовершенствовать работу. Именно поэтому необходимы пределы его использования.

Юридическая ответственность за характер деятельности механизма – удел правоприменителя. Его обязанность состоит в том, чтобы не прибегать к недозволенному, контролировать процесс в интересах обеспечения защиты прав участников правоотношения.

18. Необходима определенная форма регулирования для гарантий безопасности и полезности для общества в целом. Международно-правовое регулирование ИИ должно быть достаточно гибким, чтобы соответствовать быстро развивающемуся характеру ИИ. Поскольку ИИ продолжает развиваться и появляются новые технологии и приложения, нормативная правовая база должна быть в состоянии адаптироваться к этим изменениям и обеспечивать разработку и использование ИИ в соответствии с этическими стандартами и стандартами в области прав человека.

19. Использование ИИ в судебной системе и при отправлении правосудия имеет несколько международно-правовых аспектов, которые необходимо учитывать:

- любые системы ИИ, используемые в отправлении правосудия не должны нарушать эти права человека. Любые погрешности в данных, используемых для обучения систем ИИ, должны быть выявлены и устранены, а их влияние на разные социальные слои общества должно быть строго учтено.
- прозрачность и подотчетность означает, что процессы принятия решений любых систем ИИ, используемых в этих контекстах, должны быть открыты для проверки, а лица, ответственные за их разработку и развертывание, должны нести ответственность за любой вред, причиненный их использованием.
- конфиденциальность и защита данных означает, что любые данные, используемые системами ИИ в этих контекстах, должны собираться и использоваться в соответствии с применимыми законами о защите данных.
- использование ИИ в судебной системе и правосудии должно соответствовать этическим соображениям, включая принципы автономии, благодеяния, не причинения вреда и справедливости.

При этом, используя передовой мировой опыт необходимо обеспечить удобный и беспрепятственный доступ к правосудию через IT-сервисы; путём автоматизации процессов по обработке данных упростить и ускорить судопроизводство, сделав его более прозрачным и экономным; продолжить внедрение цифровых инструментов, направленных на повышение качества судебной защиты и усиление правозащитного потенциала силовых органов.

Технологии ИИ быстро развиваются, что может затруднить разработку правил и стандартов, которые останутся актуальными и эффективными с течением времени. Решение этих задач и проблем потребует сотрудничества и сотрудничества между политиками, юристами и техническими экспертами из разных стран. Поскольку ИИ продолжает быстро развиваться, растет потребность в международном

сотрудничестве и взаимодействии государств и международных организаций для решения юридических и этических проблем, связанных с его разработкой и внедрением.

20. Во многих странах мира наблюдается достаточно сложная криминогенная обстановка, особенно, в сфере преступлений с использованием информационных и телекоммуникационных технологий. Это требует серьезных положительных действий со стороны правоохранительных органов, в том числе, путем повышения уровня научно-технического обеспечения судопроизводства.

Для повышения качества судопроизводства на современном этапе необходимо повысить эффективность судебно-экспертной деятельности путем развития перспективных инновационных направлений судебных экспертиз.

Перспективными направлениями следует признать:

- оригинальный метод оцифровки в бинарном формате сразу всей четверки нуклеотидов в каждом «снипе», позволяющий проводить детекцию более коротких участков ДНК в старых биологических образцах». При использовании таких методов достигается максимальная цифровизация: «объем информации при ДНК-идентификации личности с помощью снипов составит для одного человека не более одного килобайта (для сравнения: с помощью ныне практикуемых STR-локусов – более 200 килобайт)»;
- внедрение в судебную почерковедческую экспертизу методов математического моделирования с программным обеспечением кодирования письменных знаков;
- идентификацию личности по динамическим признакам человека (например, походке), запечатленным на цифровом носителе с помощью камер видеонаблюдения – судебная видеопортретная экспертиза;
- психофизиологическую экспертизу с применением полиграфа. Необходимо проведение серьезной валидации с последующей сертификацией научно-обоснованной методики данного вида судебной экспертизы.

Перспективы внедрения инновационных технологий, включая искусственный интеллект, в судопроизводство будут реализовываться гораздо быстрее путем организации и систематического проведения научно-практических форумов для ознакомления с ними: съездов, симпозиумов, конференций, семинаров и других мероприятий по вопросам судебно-экспертной деятельности, с приглашением ведущих практикующих ученых-экспертов для проведения мастер-классов.

21. Вопросы правового регулирования сделок, заключенных с применением блокчейн-технологий (смарт-контракты) в отличие от электронных сделок, не могут быть урегулированы нормами

действующего законодательства.

Их специфическая структура изложения, использование компьютерного кода при написании условий сделки требует принятия отдельных норм законодательства, которое будет регулировать именно данный вид договоров.

Возможно, следует предусмотреть самостоятельную главу Особенной части Гражданского кодекса Республики Казахстан и внести изменения и дополнений в отдельные норм Общей части.

Требуется определить процедуру и порядок судебного рассмотрения споров по заключенным смарт-контрактам в случае, если одна из сторон будет неудовлетворена результатом урегулирования проблемы внутренним механизмом принудительного исполнения и расторжения договора.

22. Необходима корректировка понятия электронного документа, содержащегося в подпункте 12) статьи 1 Закона Республики Казахстан «Об электронном документе и электронной цифровой подписи».

Существующее определение является узким, и не охватывает документы, составляемые с помощью компьютерного кода, поскольку подразумевают под собой только документы в электронно-цифровой форме, подписанные с помощью электронной цифровой подписи.

Внесение соответствующих изменений и дополнений в законодательство будет способствовать более полному регулированию правоотношений в сфере заключения смарт-контрактов с применением блокчейн-технологий, а также защите прав лиц, вовлеченных в эти правоотношения.

RECOMMENDATIONS
on results of the International Scientific and Practice Conference on: «Artificial Intelligence and Big Data in Judiciary and Law Enforcement: Reality and Modern Demands»

Participants of the International Scientific and Practice Conference on: **«Artificial Intelligence and Big Data in Judiciary and Law Enforcement: Reality and Modern Demands»**, through the joint participation of experts from the scientific and educational community and representatives of law enforcement and judicial system of the Republic of Kazakhstan, Russian Federation and the Republic of Uzbekistan: *the Supreme Court of the Republic of Kazakhstan, Russian Federation, General Prosecutor's Office of the Republic of Kazakhstan, Investigative Committee of the Russian Federation, Academy of Sciences of the Republic of Kazakhstan*

Artificial Intelligence is a set of technological solutions that allows imitating human cognitive functions, for human purposes, which are solved by generating predictions, recommendations or solutions based on analysis of data and identified patterns, adapted to the environment and influencing the environment with which the artificial intelligence interacts.

Today, there is no doubt that artificial intelligence is a strategic technology that is growing thanks to increasing computing power, the accumulation of large amounts of data and the development of networks such as 5G.

Since 2018, most countries have developed and approved strategies for the development of artificial intelligence. A study of international experience shows that predicting the recidivism of offences, detecting abnormal behavior, and predicting court decisions are among the attractive areas for the development of artificial intelligence

Artificial Intelligence should not be regarded as a human substitute in criminal proceedings. It is only an additional tool to enhance its abilities, abilities and human potential, to help ensuring effectiveness of forecasting, investigation, uniformity of court practices and qualitative protection of citizens' rights.

1. Criminal justice is an activity carried out with human interaction, and, above all, it develops social technologies and forms a certain set of methods, means, techniques of such interaction, ensuring the achievement of the goals of this activity. The most successful social technologies of cognition receive procedural-legal regulation and become norms of evidentiary law.

The emergence of digital technologies and their total penetration into the sphere of social relations cannot but affect the law in general and criminal procedural cognition and evidence in particular.

Digital language is not created for free social interaction between people. It is created for "man-machine" interaction, and man creates something artificial and formally algorithmic to send commands to the machine and receive its reaction. It requires an interpreter, not an interpreter, to discover the legal meanings in such interaction. He must understand the meaning and purpose of each digital command-code; know what machine reaction it generates; be able to explain in human language the whole process of "man-machine-human" interaction.

2. Transformation of the evidence in criminal cases of computer (cyber) crime is necessary and inevitable, but it requires professional interaction and joint research of lawyers with specialists in the field of digital technology.

The result of the technologization of court proceedings will be a transition to digital court proceedings, i.e., the activities of the court, participants in the case and other actors in the process, as well as the enforcement authorities in resolving legal cases governed by procedural law, in which the key factor is digital data, the processing and use of the results of analysis compared with traditional forms of court proceedings, which significantly improves its efficiency.

The following processes seem to be the most important in this activity:

1. acquisition and transformation of information relevant for court proceedings into machine-readable information,
2. its further accumulation,
3. analysis and processing of the got information,
4. formation of a proposed solution,
5. back transformation of information into human-readable form,
6. use of obtained results.

3. Most significant in the process of application of artificial intelligence is the principle of user control, according to which, a human judge should be able to refute the proposition of artificial intelligence and make his own decision on the case, and participants of the process should be able to appeal directly to a human court (consisting of people) and challenge the decision made by the artificial intelligence.

Most of the arguments among specialists are about punishment for humans, i.e. about the nature of the decision made by the machine, consideration of the motive for the act, the presence of mitigating circumstances, including those based on the emotional state of the perpetrator. But it is equally important to understand how, on the basis of what algorithm, such a decision is made.

A human-readable draft decision must contain a reference to those factors that allowed the AI to make certain conclusions for final evaluation and human decision-making.

The work on technologization of court proceedings will require a lot of human, material, time and other resources, but there is no alternative to the way the legal community is going now, and the earlier and more actively this activity is carried out, the more effective the result will be.

4. Criminal economic, socio-political and other purposes use the latest high-tech means: from committing crimes using remote technologies to using neural network technologies and artificial intelligence.

Law enforcement efforts to analyse and exploit Big Data are clearly insufficient at present. Attempts by governments to control information on the Internet and its use for investigative and, more generally, judicial purposes are unprepared and clearly limited.

This delay in organising the widespread use of big data for judicial purposes creates the following organisational problems:

- difficulty in analysing big data;
- inaccurate prediction of criminal offence development
- lack of effective models of state response to prevent crime, etc.

Particular attention should be paid to the formation and use of big data in court proceedings. Research and development of innovative means and methods based on digital technologies, including artificial intelligence, for processing and using Big Data in practice, with their subsequent institutional and legal regulation, are relevant in this respect.

To this end, the following measures are proposed:

1. Develop organisational and legal framework for the use of Big Data in order to fully legitimise the use of Big Data in solving urgent legal applications, by including provisions for ethical requirements that regulate the formation and use of Big Data (including the database of the general genomic registration of the country's population).
2. Develop and include in the programs of professional training for investigators, police officers and court experts, as well as in the system of advanced training for judges a new section of information training - "Forensic tools and techniques for the use of Big Data (Big Data).
3. To develop expert systems based on cognitive computing with self-learning properties, including the use of well-known software samples NoSQL, MapReduce, Hadoop and neural networks. Certainly, some monetary and human resources must be allocated to carry out such work.
4. Raise the level of logistical support for the use of big data through acquisition (or own production) of Summit-class supercomputers from IBM, Fujitsu (Japan).
5. Establish highly qualified Big Data (Big Data) units in the law enforcement system, including courts, and ensure their technical ability to access such databases.
6. Increase the level of professional training of law enforcement officers to successfully implement innovative research methods.

7. To unite efforts of states in close cooperation between law enforcement agencies on the use of Big Data in legal proceedings (starting with international search for criminals and missing persons and ending with the fight against organised cybercrime) with appropriate international institutional and legal framework (adoption of international conventions, agreements and other legal regulatory instruments).

It is a comprehensive approach to institutional and legal regulation of the use of big data (Big Data) that will enhance the effectiveness of its application in court proceedings.

5. There are a number of problems faced by the traditional judicial system *(limited access to justice, the slowness of the judicial process, the uneven quality of judicial decisions and the possible impact of human factors on the outcome of a case).*

The introduction of new technologies may have positive effects on the quality and accessibility of the judicial process but also bring challenges such as the dehumanization of the law, cybersecurity issues and the need to adapt legislation and judicial infrastructure to the new technological realities.

Ensuring cyber security, developing a legal framework, adapting the traditional judicial system to the challenges of information technology and taking into account the views and experiences of all stakeholders are key aspects to be considered when introducing new technologies into the judicial system.

An important step in this direction is the adoption of the Digital Justice Code, which aims to provide a legal framework for a new transparent judicial system based on information technology and the protection of human rights.

6. The main challenges to the use of AI in judicial and law enforcement activities are highlighted.

First, ensuring trust in artificial intelligence systems applied in judicial and law enforcement activities. In turn, the problem related to ensuring trust is a potential systematic error in AI algorithms. AI systems are trained based on the data entered into them. If the data used in training contains systematic error, the AI model will also have systematic error, leading to discriminatory results.

Secondly, the issue of transparency in the use of AI in judicial and law enforcement activities. The decision-making process in AI systems is often opaque, without a clear explanation of how the system arrived at a particular decision. AI algorithms are often treated as "black boxes", which means that it can be difficult to understand how an algorithm arrived at a particular decision.

Third, the use of AI in these domains can lead to ethical problems, such as breaches of confidentiality. The training data used to build AI models often

contain personal information. AI systems can also collect personal data from individuals without their consent.

Fourth, the use of AI in judicial and law enforcement activities can lead to job losses and, as a result, social and economic problems.

With this in mind, developers are encouraged to build AI systems that can be trusted technically and psychologically.

7. The use of artificial intelligence in justice carries certain risks: what is the admissibility of evidence collected and processed by a robot machine, will such judgments, verdicts have legal force? Therefore, its implementation requires a solid scientific and practical basis. Practitioners have a lot of work to do in order to implement the innovation safely. There is a need for scenarios to respond to possible errors and violations. An in-depth revision of laws is required. Thought needs to be given to introducing new offences or qualifiers.

8. Criminal procedural and forensic activities are rapidly changing in the context of global digitalisation, Russia as well as Kazakhstan are actively involved in transformational processes. A study of Kazakhstan's experience in electronic document management and the possibility of investigating criminal cases in an "electronic" format indicates significant progress in this area, which deserves close attention.

In terms of general innovations due to the applied nature of the science of criminology, general and private innovative methods to improve the quality of training of current and future investigators in the context of global digitalization are proposed.

The general innovative methods include:

1) The use of educational audio and video production, including on websites, social networks and messengers.

2) The use of gamification technologies in forensics, the development of computer games, specialised computer programmes and mobile applications, and other e-learning resources. However, further successful development can only be ensured through collective work of lawyers and IT-specialists and with appropriate, mainly budgetary, funding.

3) Interdisciplinary applied research.

Private innovative methods of training investigators in the context of digitalisation should include:

1) Targeted development (based on the above-mentioned general methods, of modern forensic techniques of investigation of the so-called "computer" or cybercrime, as well as relevant tactics, tactical operations and combinations.

2) Issues of appointment of computer forensics, cooperation of an investigator with IT experts and specialists, relevant investigative officers and operative-technical units are urgent problems of practice.

Thus, criminalistics should constantly develop not only as the science, but also as set of interesting, accessible stated, applied recommendations, and also the similar didactic means.

9. The application of mathematical statistics and artificial intelligence made it possible to build a digital forensic model of serial crimes, containing 27 features with different numbers of gradations, as well as to identify regular relationships between the features of their system. The patterns of the offences studied determined the choice of features on the basis of which it was possible to establish the serial nature of non-obvious offences and the persons involved in them. The geographical coordinates of the crime scene, time of the act (initial and final), type of the crime scene, method and weapon, age of the victim were such features. These features have been converted into evidentiary variables. The developed software can be applied to various types of serial crimes.

Thus, the hypothesis that artificial intelligence can be used for:

a) constructing a search portrait of a serial offender;

b) identifying those in the mass of unsolved acts that are of a serial nature and committed by the same subject (identification of crime links);

c) identifying the most likely suspect from among the persons recorded in the criminal database (prioritization of the suspect).

On this basis, it is advisable to continue researching the possibilities of artificial intelligence in modelling the investigation of various types of crimes, including those of a serial nature.

10. Cybersecurity is an important component of the sovereignty of the modern state. With the dependence of states on digital technologies and the threats associated with the use of these technologies, ensuring a high level of cybersecurity becomes a necessity.

The development of appropriate infrastructure, establishment of specialised institutions, improvement of legislation and international cooperation will allow to ensure an independent policy and guarantee the resilience of society in the context of increasing cyber threats.

11. The Digital Transformation Strategy is a springboard for the development and construction of an information technology framework for cybersecurity. At the same time, the creation and search for new ways of further development and improvement of the block of information and technological basis in the system of public administration at the present stage is a priority.

The common aspiration that unites all the concepts in digital transformation is their focus on the idea of strengthening the digital space, literacy, cyber security, scientific, methodological and legal support of this process.

In this context, the main approaches and principles of building a digital transformation strategy should be

- A scientific approach and specificity, relying on modern knowledge, methodologies and technologies;
- professional approach;
- timeliness, expediency of decision-making, and anticipation of social, legal and other consequences;
- purposefulness, feasibility and rationality of actions;
- unity of all components of the digitalization development process.

12. At present, there is a tremendous increase in crimes involving the use of the Internet, including Darknet technologies. Their detection and investigation involves a number of difficulties, of which one of the most significant is:

- The specificity of the mechanism of tracing, due to the use of special software, based on algorithms of cryptographic transformation of information and various schemes of data exchange on the Internet, conditionally called "anonymizers".

In this regard, it is proposed to introduce into forensic use the term "electronic trace track", which is a system of formation of traces on the Internet, consisting of several sequentially arranged in time and logically interrelated records of the passage of computer information on communication lines through the switching equipment of communication operator(s) and (or) Internet service providers from the computer of the offender to the victim's computer or in reverse order (depending on the investigative situation).

Darknet technology itself can be defined as the processes and methods of search, collection, storage, processing, provision, distribution and protection of information on the Internet, as well as methods of implementation of such processes and methods based on the use of specialized software used to preserve the anonymity and privacy of actions carried out on the Internet.

From a forensic point of view, it seems possible to classify it into the following types:

1) search engines (Internet browsers), such as Tor (short for The Onion Router) and I2P (Invisible Internet Project, IIP, I2P);
2) operating systems like Whonix, Subgraph, Tails;
3) cloud data storage, e.g. Freenet.

13. Virtually all post-Soviet states have laid the legal foundations for the formation of a national cyber security system, mainly through the preparation and adoption of a number of normative legal acts of a conceptual nature. In addition, these documents are subject to adjustments based on the dynamics and specifics of relevant social relations.

Based on the specifics of the sphere of activity, one of the "pioneers" in terms of legal regulation of cybersecurity is the banking sector.

At the same time, the improvement of the methodology for countering cyberattacks in the banking sector involves the development of a package of information security standards, which include, among other things, requirements

- for cyber security management systems;
- on ensuring cyber security in the use of virtualization technologies;
- on cyber risk management;
- on assessment of cybersecurity compliance of banking entities with the requirements of the standards;
- documenting cybersecurity activities in accordance with the requirements of standards;
- management of cyber threats and cyber incidents;
- on ensuring cyber security of mobile software products (mobile applications).

14. To date, the impact of AI on human rights must be stated in two ways: on the one hand, great opportunities in crime prevention, prosecution and adjudication are identified, while on the other hand, threats to individual human rights violations are clearly identified.

While AI is useful, it is important to consider the potential risks and ethical implications and to ensure that it is used in a way that respects individual rights and freedoms. In this way, the benefits of this progressive technology can be harnessed while minimizing its potential harms.

To this end, several possible options are proposed to address the ethical challenges posed by the use of AI in respecting fundamental human rights:

- Developing and establishing ethical standards and guidelines prescribing the appropriate use of AI while respecting fundamental human rights;
- setting up legal and regulatory frameworks that set boundaries for the use of AI, particularly in the areas of privacy, non-discrimination and transparency;
- fostering collaboration between AI developers and human rights experts to identify potential biases, discriminatory outcomes and other ethical issues in their technologies;
- Increasing transparency about the data and algorithms used in AI systems;
- Empowering citizens to control their personal data and providing them with information on how this data is used;
- conducting regular audits of AI systems by independent third-party organizations to ensure that they are designed and used in a way that respects fundamental human rights;

- providing education and training to employees of companies using AI on its ethical use.

15. There is no clear legal regulation of the use of AI technologies. An urgent task is to define the limits and possibilities for the use of AI technologies in law enforcement practice, including the judiciary.

Following the fashion for "digital", one began to talk about digital justice, digital crime, digital policing and cyber-justice. And there are a great number of such terms nowadays. Each author understands something different under these terms, although each word has its own meaning. The same thing happened with artificial intelligence.

Intellect is a property of a living organism, given to it by nature - the human being. In other words, speaking of the artificial intellect, the property of a human being is transferred to a certain technical tool, mechanism or apparatus.

Artificial intelligence is an imitation of what programmers imagine as human intelligence. That is, they implement their idea of intelligence, not create it. It is impossible to do this. Artificial intelligence is not really intelligence in the conventional sense, but merely an imitation.

There is a need for engineers to work more closely with philologists and lawyers.

16. AI actors should make every effort to minimize discriminatory practices (discriminatory on the basis of race, gender, nationality, social origin, religion, political or other beliefs, color, age, language, birth conditions, physical disabilities and any other factors) in the life cycle of the AI system.

The phenomenological version, which treats human values as the result of the manifestation of sensual acts, is more suitable for this purpose. Orientation on phenomenological ethics will allow introducing into the artificial mind the ability to experience, to feel empathy, to distinguish bad from good deeds not on the basis of inbuilt data set, but on the basis of generally accepted norms of morality and ethics, honesty and humanism.

An AI system organized in this way will be able to function effectively in many areas of human activity, including law enforcement.

Without maintaining the principles of phenomenological ethics, "strong" artificial intelligence poses a significant danger to human civilization. It is necessary to focus efforts on creating robust artificial intelligence management systems. It should be borne in mind that the pace of AI development has far outstripped the pace of thinking about risks and threats.

17. A legal relationship is characterized by subjective legal rights and duties of the parties, which are established by the relevant legal rules. Legal relations are always a bilateral relationship. The content of legal relations consists of subjective legal rights and duties. Subjective legal right consists of

three powers: to act on one's own, to demand performance of an obligation from the other party and to claim.

Neural network software of an artificial intelligence vehicle is a result of creative activity of an individual or a group of individuals - a programmer (programmers). They are the carriers of subjective legal rights and obligations.

However, at a certain stage, the development of this software is also possible without the participation and influence of the author(s). That is, the apparatus itself can produce new information, and unpredictably so. At the same time, the technical means, apparatus, mechanism, in which the artificial intellect is contained, is not a carrier of subjective legal rights and obligations, as it does not possess the necessary qualities for this.

Legal relations in the absence of the rule of law are impossible. Therefore, in order to regulate the process of application of artificial intelligence technologies, its legal support is important.

It is necessary to work out the unified approaches to use of artificial intelligence technologies, to systematize the directions and forms of its introduction into law enforcement practice, including justice.

Certainly, the position of artificial intelligence in legal relations arising in law enforcement practice should be clearly defined. It seems that its purpose is to provide, streamline the managerial functions, organizational support for the activities of the enforcer.

The subject of the legal relations can only be a law enforcer - a human being. The mechanism, containing artificial intellect, is only an assistant, a technical means to optimize, accelerate and improve the work. This is why limits to its use are necessary.

The legal responsibility for the nature of the mechanism's activity is the duty of the enforcer. His/her duty is to avoid resorting to the unauthorized, to control the process in order to protect the rights of the participants of the legal relations

18. Some form of regulation is necessary to guarantee safety and utility for society as a whole. International legal regulation of AI must be flexible enough to accommodate the rapidly evolving nature of AI. As AI continues to evolve and new technologies and applications emerge, the legal framework must be able to adapt to these changes and ensure that the development and use of AI is consistent with ethical and human rights standards.

19. The use of AI in the judicial system and in the administration of justice has several international legal aspects that need to be considered:

- Any AI systems used in the administration of justice must not violate these human rights. Any inaccuracies in the data used to train AI systems must be identified and corrected, and their impact on different social sectors

of society must be strictly considered.

- Transparency and accountability means that the decision-making processes of any AI systems used in these contexts must be open to scrutiny, and those responsible for their design and deployment must be held responsible for any harm caused by their use.

- confidentiality and data protection means that any data used by AI systems in these contexts must be collected and used in accordance with applicable data protection laws.

- the use of AI in the judicial system and justice should comply with ethical considerations, including the principles of autonomy, beneficence, do no harm and fairness.

At the same time, using the best international experience, it is necessary to provide convenient and unhindered access to justice through IT services; simplify and speed up legal proceedings by automating data processing processes, making it more transparent and economical; continue the introduction of digital tools aimed at improving the quality of judicial protection and strengthening the human rights potential of law enforcement agencies.

AI technologies are evolving rapidly, which may make it difficult to develop rules and standards that remain relevant and effective over time. Addressing these challenges and problems will require cooperation and collaboration between policy makers, lawyers and technical experts from different countries. As AI continues to evolve rapidly, there is a growing need for international co-operation and collaboration among states and international organizations to address the legal and ethical challenges associated with its development and implementation.

20. In many countries around the world, the crime situation is quite complex, especially with regard to crimes involving information and telecommunication technologies. This requires serious positive action on the part of law enforcement agencies, including by improving the level of scientific and technical support to judicial proceedings.

In order to improve the quality of court proceedings at the present stage it is necessary to increase efficiency of forensic expertise through development of perspective innovative directions of forensic expertise.

The following should be recognized as promising areas of focus:

- The original method of digitization in binary format of all four nucleotides in each "snip" at once, allowing the detection of shorter DNA sections in old biological samples" When using such methods, maximum digitization is achieved: "the volume of information during personal DNA identification using snips will be less than one kilobyte for one person (for comparison: with the currently practiced STR-loci it will be more than 200 kilobytes)";

- Introduction of mathematical modeling methods with software for

coding of written signs into forensic handwriting expertise;

- identification of a person by dynamic human features (e.g., gait) captured on digital media through video surveillance cameras - forensic video-portrait examination;

- Psychophysiological assessment using a polygraph. Serious validation is needed, followed by certification of a scientifically based methodology for this type of forensic examination.

The prospects of implementing innovative technologies, including artificial intelligence, in court proceedings will be realized much faster through the organization and systematic organization of scientific and practical forums to introduce them: congresses, symposiums, conferences, seminars and other events on issues of forensic expertise, inviting leading practicing scientists-experts to conduct master classes.

21. Issues of legal regulation of transactions concluded with the use of blockchain technologies (smart contracts), unlike electronic transactions, cannot be regulated by the norms of the current legislation.

Their specific structure and the use of computer code in writing the terms of the transaction require the adoption of separate rules of law which will regulate this particular type of contract.

Probably it is necessary to provide a separate chapter of the Special Part of the Civil Code of the Republic of Kazakhstan and to make changes and additions to separate norms of the General Part.

It is required to determine the procedure and order of judicial consideration of disputes on the concluded smart contracts in case one of the parties is unsatisfied with the result of settlement of the problem by the internal mechanism of compulsory execution and termination of the contract.

22. It is necessary to adjust the concept of an electronic document contained in sub-paragraph 12) of Article 1 of the Law of the Republic of Kazakhstan "On Electronic Document and Electronic Digital Signature".

The existing definition is narrow and does not cover documents made by means of computer code, as it implies only documents in electronic digital form signed by means of electronic digital signature.

The introduction of relevant amendments and additions to the legislation will contribute to a fuller regulation of legal relations in the area of conclusion of smart contracts using blockchain technologies, as well as protection of the rights of the persons involved in these legal relations.

Мақалалар авторлық редакцияда басылды. Мақала мазмұнына ұйымдастырушылар жауапты емес.

Статьи даны в авторской редакции. Оргкомитет не несет ответственности за содержание работ.

Қазақстан Республикасының Бас прокуратурасы жанындағы Құқық қорғау органдары академиясының баспаханасында шығарылған. Таралымы 50 дана.

Отпечатано в типографии Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. Тираж 50 экз.

ISBN 978-601-7969-86-8