Вопросы безопасности
Правильная ссылка на статью:
Горян Э.В. — Этическое регулирование искусственного интеллекта как фактор информационной безопасности: опыт Таиланда // Вопросы безопасности. – 2022. – № 3. DOI: 10.25136/2409-7543.2022.3.38626 EDN: RMFIRR URL: https://nbpublish.com/library_read_article.php?id=38626

Этическое регулирование искусственного интеллекта как фактор информационной безопасности: опыт Таиланда

Горян Элла Владимировна

ORCID: 0000-0002-5962-3929

кандидат юридических наук

доцент, Владивостокский государственный университет экономики и сервиса

690014, Россия, Приморский край, г. Владивосток, ул. Гоголя, 41, каб. 5502

ella-gorjan@yandex.ru

Статья из рубрики "Компаративный анализ систем безопасности"

DOI:

10.25136/2409-7543.2022.3.38626

EDN:

RMFIRR

Дата направления статьи в редакцию:

11-08-2022

Дата публикации:

18-08-2022

Аннотация: Объектом исследования являются отношения в сфере этического регулирования применения технологий искусственного интеллекта. Предмет исследования представлен нормативными документами Таиланда, устанавливающими предписания к проектированию, разработке, исследованию, обучению, развертыванию и применению технологий искусственного интеллекта. Выделяются особенности тайского подхода к регулированию отношений в рассматриваемой сфере. Определяются субъекты, задействованные в регуляторном механизме искусственного интеллекта. Исследуются этические требования к применению технологий искусственного интеллекта применительно к отдельным категориям субъектов. Прослеживается взаимосвязь этического регулирования технологий искусственного интеллекта и обеспечения безопасности в информационном пространстве. Характеризуется национальная модель этического регулирования искусственного интеллекта. Таиланд реализует государственно-центристскую модель этического регулирования искусственного интеллекта, в рамках которой государство определяет базовые этические принципы

искусственного интеллекта и подробно регламентирует направления деятельности субъектов государственного и частного секторов по каждому из этих принципов. Особенностью тайской модели является акцент на важности подготовки и повышения квалификации государственных служащих, способных использовать цифровые технологии в управленческих процессах и эффективно реализовывать этические принципы в ходе выполнения своих функций. Таиланд включил пользователей искусственного интеллекта в круг субъектов, ответственных за реализацию этических требований, в качестве активных участников регуляторных процессов, способных оперативно влиять на содержание алгоритмов путем предоставления необходимой информации операторам искусственного интеллекта. Тайская модель рассчитана на воспитание не пассивного, а активного пользователя цифровых технологий, которому рекомендуется повышать осведомленность и улучшать навыки их использования, что приводит к усилению правового статуса пользователей с помощью инструментов «мягкого права». Реализация Таиландом своей модели этического регулирования искусственного интеллекта положительно отразится на обеспечении информационной безопасности.

Ключевые слова: персональные данные, информационная безопасность, этика, безопасность данных, критическая информационная инфраструктура, Таиланд, АСЕАН, цифровая экономика, финтех, национальная безопасность

Введение. В наши дни технологии искусственного интеллекта (далее – ИИ) играют важную роль в различных аспектах человеческой деятельности: Siri, Alexa и Google Assistant в смартфонах, технология автопилотирования автомобилей Tesla, ленты социальных сетей и музыкальных сервисов, список рекомендаций на YouTube, карты загруженности автодорог сервисов Yandex.Карты и Google Maps, - это всего лишь несколько примеров применения ИИ-технологий. Активно используется ИИ в финансово-банковском секторе, страховании, авиации и военной промышленности, медицине и правоохранительной деятельности.

Искусственный интеллект является частью инструментария обработки и принятия решений или может быть основной технологией производственного процесса, что грозит изменениями в экономике и на рынке занятости. Негативным фактором использования ИИ-технологий является непредсказуемость решений и последствий их применения. Поэтому установление внятных и однозначных ориентиров в отношении использования ИИ-технологий – одна из задач государства.

Правительство, научное сообщество и промышленные круги пришли к единому мнению, что безопасность приложений с использованием технологий ИИ становится ключевым фактором их применения, поэтому на государственном уровне необходимо принятие гарантий для снижения потенциальных рисков, связанных с ИИ [1]. С этой целью частный и публичный секторы разрабатывают каталоги этических принципов ИИ, соблюдение которых в существующих системах и продуктах ИИ сопряжено с необходимостью наличия высокотехнологичных систем управления ИИ, включая его обучение, тестирование и проверку безопасности. Эти системы управления все еще находятся на стадии интенсивной разработки, поэтому недостаточно готовы к широкому коммерческому внедрению. Основные технические препятствия глубоко уходят корнями в фундаментальные проблемы современных исследований ИИ, такие как моральное познание на уровне человека, этические рассуждения на основе здравого смысла и междисциплинарная разработка этики ИИ. Тем не менее, некоторые государства на

правительственном уровне определяют фундаментальные этические принципы, в рамках которых необходимо развивать и применять технологии ИИ.

Исследователи отмечают, что на фоне глобальной конкуренции за использование возможностей, предоставляемых искусственным интеллектом, многие страны и регионы открыто участвуют в «гонке за ИИ» [2]. По их мнению, повышенная прозрачность рисков, связанных с технологией ИИ, привела ко все более громким призывам к регулирующим органам не ограничиваться преимуществами, а также обеспечить надлежащее регулирование для обеспечения «заслуживающего доверия» ИИ, то есть законного, этичного и надежного. Помимо минимизации рисков, такое регулирование могло бы способствовать внедрению ИИ, повысить правовую определенность и, следовательно, также способствовать продвижению позиций стран в гонке. Следовательно, по мнению исследователей, «гонка за ИИ» также порождает «гонку за регулированием ИИ» [2].

Вслед за Китаем [1] и Сингапуром [3] к регулированию ИИ-технологий приступил и Таиланд, оспаривающий лидерство Сингапура в АСЕАН в сфере информационной безопасности и финтеха, выступая с инициативами унификации стандартов информационной безопасности и предлагая свою инфраструктуру и ресурсы для международных проектов [4]. Таиланд проводит активное наращивание нормативно-правовой базы для регулирования процессов кибербезопасности. В течение трех лет с 2017 по 2019 годы были приняты Национальная стратегия кибербезопасности 2017–2021 (National Cybersecurity Strategy 2017-2021), Закон о защите персональных данных (Personal Data Protection Act 2018) и Закон о кибербезопасности (Cybersecurity Act 2019). С целью упорядоченного развития отрасли финтеха были приняты План развития цифрового правительства на 2020-2022 годы (Digital Government Development Plan 2020-2022, URL: https://www.dga.or.th/wp-content/uploads/2021/09/□□□□□□□□□□□□□□□□□□□□□□□□□□□-□.□.-2563-2565-□□□□□□□□□.pdf) и подготовленное Министерством цифоровой экономики и общества Таиланда Руководство по этике искусственного интеллекта (AI Ethics Guideline, URL: https://www.etda.or.th/getattachment/9d370f25-f37a-4b7c-b661-48d2d730651d/Digital-Thailand-AI-Ethics-Principle-and-Guideline.pdf.aspx?lang=th-TH).

Этические требования к технологиям ИИ и соответственно продуктам и услугам их использующим имеют целью обезопасить информационно-технологическую сферу, исключить нарушение прав и законных интересов субъектов. Несомненно, ИИ используется для облегчения и ускорения технических процессов и минимизации производственных затрат, что приносит пользу одновременно и операторам ИИ, и пользователям продуктов и услуг. Но, с другой стороны, возникают риски злоупотребления этими технологиями как операторами, так и третьими лицами, незаконно вмешивающимися в процессы. Нельзя забывать и о рисках получения дискриминационных/несправедливых решений ИИ в случае недоработки алгоритмов и уязвимости целостности процессов. Эти факторы влияют на общее состояние безопасности информационных систем. Поэтому этическое регулирование ИИ в перспективе отражается на информационной безопасности той или иной отрасли сферы, будь то финансово-банковского сектора или здравоохранения. Кроме того, применение ИИ-технологий в объектах критической информационной инфраструктуры требует осторожного подхода как в техническом, так и организационно-правовом аспектах. Вышесказанное и определяет актуальность нашего исследования.

Цель исследования – определить особенности подхода Таиланда к этическому регулированию использования технологий искусственного интеллекта в аспекте

информационной безопасности. С целью получения наиболее достоверных научных результатов был использован ряд общенаучных (системно-структурный и формально-логический методы) и специальных юридических методов познания (сравнительно-правовой и формально-юридический методы).

Предмет исследования составляют основные программные и нормативно-правовые акты Таиланда в сфере регулирования ИИ-технологий, а также ряд научных исследований по теме.

Выбранная нами для исследования тема еще не представлена в российской научной литературе и является логическим продолжением нашего исследования в рамках гранта РФФИ «Обеспечение прав инвесторов в банковском и финансовом секторах в условиях цифровизации экономики в РФ и ведущих финансовых центрах Восточной Азии: сравнительно-правовой аспект». Из зарубежных исследований следует отметить две ключевые работы. В 2008 году была опубликована статья, посвященная этическим вопросам и политическим последствиям внедрения информационных технологий в систему национальной безопасности Таиланда [5]. Ценность этого исследования заключается в том, что она стала первой попыткой пролить свет на «запрещенную» в Таиланде тему путем сравнения опыта США и Таиланда. По мнению автора, американская модель национальной безопасности оказывает значительное влияние на подход таиландской разведки и применение информационных технологий в системе национальной безопасности, в то время как оба разведывательных сообщества имеют схожие проблемы с разведкой и вызывают этические дебаты о нарушениях прав человека. Вторая статья увидела свет в 2021 году: автор проанализировал Руководство по этике искусственного интеллекта в свете политических событий и общественных трансформаций [6]. По мнению автора, с одной стороны, Таиланд пытается влиться в ряды более развитых экономик, но, с другой стороны, у законодателя наблюдается сильное желание сохранить собственные традиционные ценности. Таиланду пока не удалось разрешить эту дилемму, и это прослеживается в содержании документа.

Основная часть. Искусственный интеллект меняет рынки труда как в развитых, так и в странах с развивающейся экономикой, вызывая опасения беспрецедентного сокращения рабочих мест. ИИ-технологии уже широко применяются во всех секторах и отраслях экономики: от юриспруденции и медицины до бухгалтерского учета, цифрового производства и туризма. Некоторые отрасли особенно уязвимы для автоматизации, например, промышленное производство и аутсорсинг бизнес-процессов (BPO). В странах с развивающейся экономикой, в которых представлена значительная рабочая сила в этих областях, растет призыв к упреждающим действиям, чтобы свести к минимуму потерю рабочих мест и использовать предоставляемые технологиями возможности по созданию рабочих мест. Поэтому правительства должны быть заинтересованы в правильном использовании ИИ-технологий и связанных с ними инструментов автоматизации для укрепления международной конкурентоспособности национального производителя, улучшения качества государственных услуг и развития новых видов бизнеса.

В Таиланде власти заняты разработкой эффективных мер, которые позволят им использовать упомянутые возможности и минимизировать риски. Выделено несколько стратегических технологических направлений цифровизации государственного управления (Digital Government Development Plan 2020-2022, URL: https://www.dga.or.th/wp-content/uploads/2021/09/□□□-□.□.-2563-

2565-□□□□□□□□□.pdf): (1) применение технологий виртуальной реальности (VR) и дополненной реальности (AR) при моделировании среды или ситуаций с целью регулирования/управления общественной безопасностью, телемедицины, новых форматов образования и туризма; (2) обработка больших данных и создание прогнозов и оценок в бизнес-среде с использованием технологий интернета вещей (Internet of Things, IoT) и Smart Machine для выполнения анализа ответов пользователей в режиме реального времени; (3) применение технологии Advanced Geographic Information System в управлении географическими данными, а также ее применение в управлении сельскохозяйственными ресурсами, транспортной системой и другими областями; (4) раскрытие информации и предоставление данных для пользователей путем обновления баз данных и веб-сайтов для обеспечения более широкого доступа общественности к информации; (5) применение технологии Smart Machine для управления автоматизированными услугами и реагирования на них (система Smart Machine будет постепенно развиваться и, следовательно, сможет оценивать и решать проблемы по всей цепочке предоставления услуг); (6) решение проблем кибербезопасности путем установления стандартов кибербезопасности, пересмотра соответствующих правил с целью их совершенствования; (7) применение технологии блокчейн (block chain) для хранения данных и использования сети с целью проверки и уменьшения количества посредников в надежной среде безопасности; (8) применение технологии облачных вычислений для хранения данных для упрощения установки системы, снижения затрат на обслуживание системы и экономии инвестиций в создание сетей; (9) использование технологии IoT для облегчения преобразования государственных услуг в цифровые форматы, и в то же время технология IoT может также поддерживать работу правительства в области связи, использования мобильных технологий, анализа больших данных и сотрудничества с бизнес сектором; (10) подготовка кадров, владеющих навыками в цифровой сфере, и обучение государственных служащих улучшению государственных услуг за счет эффективного использования цифровых технологий с эффективным управлением.

Руководство по этике искусственного интеллекта (далее – Руководство) устанавливает шесть этических принципов ИИ: 1) конкурентоспособность и устойчивое развитие; 2) соблюдение законов, этики и международных стандартов; 3) прозрачность и подотчетность; 4) безопасность и конфиденциальность; 5) равенство, разнообразие, инклюзивность и справедливость; 6) надежность. Все субъекты, имеющие отношение к ИИ-технологиям, разбиты на три группы: это государственные (регулирующие) органы, операторы ИИ-технологий (разработчики, проектировщики, исследователи, производители, поставщики) и пользователи. Для первых двух разработаны отдельные предписания по реализации этих принципов в их деятельности. Рассмотрим, как должен быть реализован каждый из этических принципов.

Конкурентоспособность и устойчивое развитие.

Государственные (регулирующие) органы должны анализировать и оценивать исследования, разработки и применение ИИ в аспекте пользы для человека, общества и окружающей среды с последующей поддержкой наиболее перспективных проектов и стимулированием сотрудничества между заинтересованными сторонами. Необходимо создать цифровую инфраструктуру, аккумулирующую знания о технологиях и механизмах ИИ, а также отслеживать и контролировать использование ИИ-технологий с целью недопущения отрицательного влияния на процессы. Регулирующие органы должны разработать политику поддержки как государственных, так и частных субъектов, стимулировать инновации в области ИИ, позволяющие создать новую отрасль, а в

дальнейшем её продвигать и поддерживать. Особое внимание требуется продвижению образовательных проектов для распространения знаний об ИИ среди широких слоев населения. С целью противостояния потенциальным угрозам ИИ важно строить партнерские отношения с национальными, региональными и международными акторами и принимать участие в разработке нормативных основ ИИ в соответствующих масштабах.

Операторы ИИ-технологий должны иметь необходимые знания и понимание процессов ИИ-технологии в той части. Важно представлять преимущества, которые дает использование конкретной ИИ-технологии человеку, социальной, экономической и экологической сферам жизнедеятельности. Необходимо уменьшить различные риски, которые могут возникнуть из-за использования ИИ-технологии. Проектирование, разработка и внедрение ИИ должно происходить с учетом преимуществ, приобретаемых заинтересованными сторонами и окружающая среда, а также с возможностью модификации его работы.

Соблюдение законов, этики и международных стандартов.

На государственные (регулирующие) органы возложена обязанность поощрять образование для повышения осведомленности и понимания в области ИИ и его влияния на пользователей, а также поддерживать исследования в аспекте ИИ и прав человека. Должны быть приняты нормативные предписания, касающиеся закупок разработчиками и поставщиками ИИ-технологий, безопасности персональных данных, права на частную жизнь, конфиденциальности и других прав человека. Нужно поддерживать разработку и внедрение международно признанных стандартов и лучших практик (Best Practice), и обеспечить сертификацию (лицензирование) деятельности разработчиков и поставщиков услуг в сфере ИИ. Важным шагом в этом направлении является поддержка создания общественных организаций, осуществляющих общественный и профессиональный контроль за операторами ИИ, а также создание системы юридического консультирования операторов ИИ по поводу правовых последствий их деятельности, этики и прав человека.

Операторам ИИ-технологий необходимо разработать меры для оценки, уменьшения и недопущения правовых и этических рисков нарушения прав и свобод человека, негативного воздействия на общество и окружающую среду. Любые действия в отношении ИИ-технологий должны осуществляться в соответствии с разработанными этическими принципами. Следует проводить этическую оценку исследований, проектирования, разработки, обслуживания и использования ИИ-технологий, результаты которой должны быть представлены заинтересованным сторонам. Должна быть проведена оценка рисков воздействия исследований, проектирования, разработки, обслуживания и использования ИИ-технологий с нарушениями принципов этики. ИИ-технологии должны быть спроектированы таким образом, чтобы обеспечить возможность вмешательства человека на каждом этапе принятия решения и способность человека контролировать все действия ИИ, включая возможность регулировки.

Прозрачность и подотчетность.

Регулирующие органы в сфере ИИ должны пересмотреть прозрачность моделей и алгоритмов, используемых операторами ИИ, в аспекте соответствия им принципу объяснимости: алгоритмы, используемые в продукте/услуги, должны быть понятны, легко объяснимы и прогнозируемы, равно как и методы обучения ИИ. Этот тезис должен быть заложен в основу разрабатываемых регуляторами политик, технических стандартов и правил. Необходимо разработать механизм для обеспечения подотчетности оператора

ИИ на протяжении всего жизненного цикла системы. Такой механизм должен предусматривать внутренний и внешний аудит. Отчет об аудите должен обязательно содержать пункты об оценке рисков; действиях по их уменьшению или предотвращению; отрицательном воздействии ИИ-технологий на человека и окружающую среду, а также о лице, ответственном за расследование и устранение причины такого воздействия.

Операторы ИИ-технологий должны обеспечить доступ к массивам данных, используемым ИИ, и предусмотреть возможность ограничения используемых алгоритмов и процессов. В противном случае алгоритмы действия ИИ должны быть объяснены, а заинтересованные стороны проинформированы о причинах принятия того или иного решения. Пользователи должны быть проинформированы о том, что взаимодействуют с искусственным интеллектом, и понимать, что результат решений зависит от искусственного интеллекта. Алгоритмы должны отслеживаться, а результаты должны заноситься с журнал аудита. Периодически должна проводиться диагностика методов сбора данных, массивов данных, алгоритмов и процессов принятия решений.

Безопасность и конфиденциальность.

Государственные (регулирующие) органы должны разработать политики и технические стандарты безопасности, защиты персональных данных и конфиденциальности для сведения к минимуму уязвимости угрозы от ИИ. Важно предусмотреть требование раскрытия информации, имеющей значение для безопасности жизни, здоровья, окружающей среды. Регуляторные органы в сфере ИИ должны внедрить систему управления рисками, определить методы управления рисками и внутреннего контроля, а также их пересмотра и улучшения на регулярной основе на протяжении всего жизненного цикла системы, в том числе при необходимости демонтажа системы. Частота таких мероприятий - не реже одного раза в год или при значительных изменениях в ИИ-технологии. На государственном уровне должен быть разработан, согласован и внедрен план надзора, мониторинга и управления рисками в долгосрочной перспективе: это позволит подготовиться к появлению искусственного интеллекта, способного к постоянному самосовершенствованию (рекурсивный самоулучшающийся ИИ). Необходимо поощрять и поддерживать сотрудничество на разных уровнях, а также предусмотреть возможность разработки интегрированного ИИ на уровне организации, страны, региона. Следует отличать «нежелательные» ИИ-технологии (способные причинить вред человеку) и поддерживать обмен знаниями и опытом надзора с тем, чтобы справиться с негативным воздействием ИИ-технологий.

Операторам ИИ-технологий следует проектировать, разрабатывать и предоставлять услуги по обеспечению безопасности и защиты информационных систем от угроз и нежелательных приложений. Особое внимание следует уделить защите персональных данных, жизни и здоровью человека, а также окружающей среде. ИИ-технологии, используемые для обработки персональных данных, должны использовать принципы законности (lawfulness) и справедливости (fairness), а также иметь определенную цель обработки, соблюдать требование пропорциональности обработки данных и конфиденциальности. Сделан специальный акцент на необходимости соблюдения Закона о защите персональных данных (Personal Data Protection Act 2018), в частности, в отношении объема данных, информирования субъекта данных, анонимизиции и удаления персональных данных и т.д. Субъекты критической информационной инфраструктуры, имеющие дело с ИИ-технологиями, должны ориентироваться на требования Закона о кибербезопасности (Cybersecurity Act 2019) и обеспечивать устойчивость систем к атакам, будучи готовыми в применению запасного плана восстановления системы после различных проблем (fallback plan).

Равенство, разнообразие, инклюзивность и справедливость.

Государственные (регулирующие) органы должны устанавливать, продвигать и поддерживать руководящие принципы применения ИИ-технологий, поощрять их разнообразие в зависимости от типов и сценариев использования. Регулятор в сфере ИИ должен поощрять создание открытой платформы ИИ с целью избегания монополии, способствующей замедлению развития. Антипомонопольное законодательство должно противодействовать использованию ИИ-технологий с целью подавления конкуренции как в региональном, так и в промышленном масштабе. Необходимо продвигать и поддерживать равные возможности доступа к образованию, продуктам, услугам и сопутствующим технологиям в сфере ИИ. Потенциальные пользователи должны поощряться к более активному использованию продуктов и услуг, оснащенных технологиями ИИ.

Операторы ИИ-технологий должны исследовать, проектировать и разрабатывать ИИ-технологии с учетом потребностей и ожиданий пользователей, учитывая все социальные категории, в том числе уязвимые группы лиц (меньшинства, пожилые люди, лица с ограниченными возможностями). Заинтересованные лица, интересы которых могут быть затронуты предвзятостью и несправедливостью решений ИИ-технологий, должны быть вовлечены в процесс проектирования и разработки таких ИИ-технологий. Необходимо проводить мониторинг и своевременно исправлять неоперационные систематические ошибки (приводящие к принятию предвзятых решений). Для обучения, тестирования и проверки ИИ следует использовать различные наборы данных: это позволит обнаружить возможные систематические ошибки для каждого набора данных. При разработке ИИ-технологий необходимо соблюдать существующие международные стандарты и рекомендации, такие как ISO 40500:2012 (W3C Web Content Accessibility Guidelines 2.0 и W3C Web Content Accessibility Guidelines 2.1). Следует использовать инструменты для проверки склонности искусственного интеллекта к принятию предвзятых решений (инструменты обнаружения предвзятости), а при тестировании проверить результаты при использовании данных, которые не были включены в обучающие массивы данных. К участию в тестировании задач и процессов ИИ-технологий необходимо привлекать лиц с ограниченными возможностями, что даст возможность получать результаты, соответствующие потребностям и ожиданиям таких пользователей в будущем. Разработка и обслуживание ИИ должны основываться на принципе социальной справедливости: равный доступ к ИИ-технологиям, используемым в продуктах и услугах, должны иметь все пользователи независимо от возраста, пола, расы и других отличий.

Надежность.

Государственные (регулирующие) органы должны разработать регламенты, установить критерии и процессы для оценки качества и надежности массивов данных и моделей ИИ на постоянной основе путем анализа данных и отзывов пользователей с последующим изменением модели ИИ в сторону улучшения. Следует разработать политику и процедуры для проверки каналов связи с пользователями и проводить регулярные проверки для получения необходимой информации. Параллельно нужно поддерживать исследования, проектирование, разработку, обслуживание и использование надежных технологий искусственного интеллекта. Руководящие принципы оценки качества и надежности ИИ должны разрабываться совместно с заинтересованными представителями государственного и частного сектора.

Операторы ИИ-технологий должны определить методы исследования ИИ. Они должны быть четко определены для каждого этапа: методы проектирования, методы разработки и

методы использования. Они должны применяться систематически и всеобъемлюще. Необходимо знать и понимать факторы, влияющие на качество массивов данных, используемых в ИИ, такие как точность (accuracy), полнота (completness), достоверность (veracity), обновляемость (update), релевантность (relevance), целостность (integrity), удобство использования (usability) и вмешательство человека (human intervention). Особое внимание следует уделить технологиям, имеющим доступ к массивам данных, имеющих конфиденциальный характер (врачебная тайна, персональные данные, финансовая (банковская) тайна, данные о юридической/правоохранительной деятельности). Тестирование моделей ИИ следует проводить в соответствии с динамикой фактических условий на предмет безопасности для пользователей и окружающей среды. Поставщики ИИ-технологий должны организовать каналы обратной связи, чтобы пользователи могли сообщать о проблемах, а также канал запроса на пересмотр решений, принятых системой.

Руководство предусматривает комплекс гарантий прав пользователей продуктов и услуг, оснащенных ИИ-технологиями. Такие гарантии коррелируют обязанностям операторов ИИ по этическому использованию ИИ и обеспечивают права уязвимой в технологическом отношении стороны. В частности, пользователи должны повышать свой уровень знаний и навыков использования продуктов и услуг с ИИ, иметь представление о преимуществах ИИ-решений. Важно следить за новостями, связанными с ИИ-технологиями, чтоб быть в курсе о возможных угрозах. Следует проверять надежность продуктов и услуг с ИИ, а также сертификатов, выданных уполномоченными организациями. Необходимо знакомиться с дизайном и принципами работы ИИ, запрашивать у поставщиков услуг подробную информацию об этических принципах, используемых в продуктах и услугах с ИИ. При возникновении проблем с использованием продуктов и услуг пользователи должны сообщить поставщику услуг всю необходимую информацию для улучшения, исправления и развития ИИ-технологии в соответствии с поставленными задачами. От исследователей, дизайнеров и поставщиков услуг необходимо запрашивать объяснение об алгоритме и принципах работы технологии, чтобы исключить возможность появления ошибочных и предосудительных результатов. В случае использования персональных данных для исследования, проектирования, разработки и предоставления услуг ИИ пользователи имеют права в соответствии с Законом о защите персональных данных (Personal Data Protection Act 2018) сделать запрос и получить информацию о массиве данных, который используется операторами ИИ. Гарантируется право отзыва согласия на сбор, использование или раскрытие информации, а такаже возразить против таких действий оператором, в том числе потребованить удаления/уничтожения или временного приостанавления использования персональных данных.

Выводы. Подводя итоги вышесказанному, отметим следующие особенности подхода Таиланда к этическому регулированию использования технологий искусственного интеллекта в аспекте информационной безопасности. Таиланд реализует государственно-центристскую модель, в рамках которой государство определяет базовые этические принципы ИИ и подробно регламентирует направления деятельности субъектов государственного и частного секторов по каждому из этих принципов. В отличие от двухуровневой модели этического регулирования ИИ, разработанной в Китае, тайская модель включает всего лишь один набор общих принципов. В совокупности со сжатыми (2 года) планами цифровизации государственного управления и экономики с выделением стратегически важных отраслей и сфер деятельности такая модель видится обоснованной. Особенностью тайской модели является акцент на важности подготовки и повышения квалификации государственных служащих, способных использовать цифровые технологии в управленческих процессах. Это позволит им эффективно

реализовывать этические принципы ИИ в ходе выполнения своих функций. Выделение государственных (регулирующих) органов в качестве субъекта, ответственного за развертывание ИИ-технологий, и наделение их соответствующими обязанностями в сфере этического регулирования, является дополнительной гарантией обеспечения информационной безопасности. Заслуживает внимания включение Таиландом пользователей продуктов и услуг с ИИ-технологиями в круг субъектов, ответственных за реализацию этических требований к ИИ: пользователи привлекаются в качестве активных участников регуляторных процессов, способных оперативно влиять на содержание алгоритмов путем предоставления необходимой информации операторам ИИ. Тайская модель рассчитана на воспитание не пассивного, а активного пользователя цифровых технологий, которому рекомендуется повышать осведомленность и улучшать навыки их использования, что приводит к усилению правового статуса пользователей с помощью инструментов «мягкого права». Можно предположить, что реализация Таиландом своей модели этического регулирования искусственного интеллекта положительно отразится на обеспечении информационной безопасности.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 20-011-00454 «Обеспечение прав инвесторов в банковском и финансовом секторах в условиях цифровизации экономики в РФ и ведущих финансовых центрах Восточной Азии: сравнительно-правовой аспект».

Библиография

1. Горян Э.В. Этическое регулирование искусственного интеллекта как фактор безопасности финансово-банковского сектора: опыт Китая // Вопросы безопасности. 2022. № 2. DOI: 10.25136/2409-7543.2022.2.38380.
2. Smuha N.A. From a ‘race to AI’ to a ‘race to AI regulation’: regulatory competition for artificial intelligence // Law, Innovation and Technology. 2021. №1(13). Pp. 57-84.
3. Горян Э.В. Перспективы использования искусственного интеллекта в финансово-банковском секторе: опыт Сингапура // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2020. Т. 12, № 3. С. 86–99.
4. Горян Э.В. Нормативно-правовой механизм обеспечения безопасности киберпространства Таиланда // Вопросы безопасности. 2021. № 3. С. 1-20. DOI: 10.25136/2409-7543.2021.3.36255
5. Kitiyadisai K. Information systems for national security in Thailand: ethical issues and policy implications / Journal of Information, Communication and Ethics in Society. 2008. Vol. 6. №2. Pp. 141-160/
6. Hongladarom S. The Thailand national AI ethics guideline: an analysis // Journal of Information, Communication and Ethics in Society. 2021. Vol. 19. №4. Pp. 480-491.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования. Предметом исследования рецензируемой статьи "Этическое регулирование искусственного интеллекта как фактор информационной безопасности: опыт Таиланда" являются этические нормы, применяемые в Таиланде, регулирующие вопросы применения искусственного интеллекта, и обеспечивающие информационную

безопасность в обществе.

Методология исследования. Автором при подготовке статьи применялись многие современные методы научного познания. Главный метод - это сравнительный анализ. Без изучения зарубежного опыта и использования сравнительного правоведения, позволяющего избегать повторения ошибок в отечественном законодательстве и судебной практике, трудно оценить эффективность решения проблем права и правоприменения по вопросам правового положения (режима) искусственного интеллекта в России. Кроме того, автором использовалось сочетание теоретической и эмпирической информации. В целом применение современных методов научного познания позволило автору изложить материал последовательно, грамотно и ясно.

Актуальность исследования. Следует полагать, что изучение прогрессивных положений зарубежного права действительно будет способствует совершенствованию собственного законодательства, поскольку позволяет не только разглядеть самобытность и историческую правопреемственность, но и выяснить, обладают ли положения о правовом статусе (режиме) искусственного интеллекта, как нового правого явления, общими чертами, характеризующими как особая ценность в информационном обществе, и насколько допустимо иностранное заимствование при формировании собственной правовой системы без ущерба ее уникальности и индивидуальности. Использование зарубежного опыта обнаруживает массу вопросов и коллизий, требующих разрешения применительно к национальному праву. На что и указывает автор рецензируемой статьи. Различные цифровые технологии, применяемые в информационном обществе, требуют правильного подхода в правовом регулировании. Глобальная цифровизация общественных отношений нуждается в адекватном правовом регулировании. Именно по этим обстоятельствам важен зарубежный опыт правового регулирования.

Научная новизна. Бесспорно, статья на тему "Этическое регулирование искусственного интеллекта как фактор информационной безопасности: опыт Таиланда" является новой для российской юридической науки, отсутствуют фундаментальные исследования по этой теме. Такая ситуация объясняется новизной самого института искусственного интеллекта и только недавно начавшимся формированием правовых норм, регулирующих общественные отношения, предметом которых является искусственный интеллект. Более того, научные споры о возможности признания искусственного интеллекта субъектом права вносят еще больше неопределенности в решение этого вопроса.

Стиль, структура, содержание. Статья написана научным стилем, структурирована, содержание статьи раскрывает заявленную автором тему.

Библиография. На наш взгляд, автору следовало бы изучить труды российских ученых, которые занимаются вопросами правового положения искусственного интеллекта (А.В. Минбалеев, Т.А. Полякова, В.Б. Наумов, Е.В. Виноградова, Т.Я. Хабриева и др.). От освещения общетеоретических вопросов статья бы только выиграла. Хотя отмеченное замечание не умаляет проделанной автором работы. Полагаем, что тема статьи является слишком узкой, и именно поэтому количество источников незначительно. Хотя общепринятым требованием для научных статей является использование не менее 15 источников, включая публикации последних лет.

Апелляции к оппонентам. Обращение автора рецензируемой статьи к оппонентам весьма корректно.

Выводы, интерес читательской аудитории. Статья "Этическое регулирование искусственного интеллекта как фактор информационной безопасности: опыт Таиланда" в целом (за исключением замечания по библиографии) отвечает требованиям, предъявляемым к публикациям подобного рода. Статья рекомендуется для опубликования в научном журнале "Вопросы безопасности". Исходя из актуальности темы статьи, она может быть интересна не только специалистам в области

информационного права и информационной безопасности, но и широкому кругу читателей.