Вопросы безопасности
Правильная ссылка на статью:
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 URL: https://nbpublish.com/library_read_article.php?id=36255

Нормативно-правовой механизм обеспечения безопасности киберпространства Таиланда

Горян Элла Владимировна

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 "Правовое обеспечение национальной безопасности"

DOI:

10.25136/2409-7543.2021.3.36255

Дата направления статьи в редакцию:

10-08-2021

Дата публикации:

04-09-2021

Аннотация: В качестве объекта исследования выбраны правовые отношения, возникающие при осуществлении мер по обеспечению кибербезопасности. Характеризуются положения нормативно-правовых актов Таиланда в сфере кибербезопасности. Исследуются особенности программных и регулирующих документов: Национальной стратегии кибербезопасности Таиланда 2017–2021, Политики и плана национальной безопасности (2019-2022), Закона о компьютерных преступлениях 2007 года (в редакции от 2017 года), Уголовного кодекса 1956 года (в редакции 2019 года), Закона о защите персональных данных 2017 года и Закона о кибербезопасности 2019 года. Определяются особенности нормативно-правового механизма обеспечения безопасности киберпространства Таиланда. Таиланд в своих программных документах не определяет основные информационные угрозы во внутренней и внешней сфере вместе с приоритетами развития системы кибербезопасности, а всего лишь очерчивает круг национальных интересов и ставит задачи, выполнение которых способно вывести его в лидеры региона. Законы разработаны с учетом последних тенденций в сфере информационных технологий и включают в сферу регулирования такие вопросы как защита персональных данных, компьютерных и информационных систем, критически важной информационной инфраструктуры. Законодательно установлена вертикаль государственного управления и мониторинга, очерчен круг полномочий компетентных органов. В сфере защиты персональных данных законодательство Таиланда в

значительной мере дублирует положения Общего регламента по защите данных Евросоюза. Отличительной чертой нормативно-правовых актов является легальное обоснование ограничения прав и свобод человека при реализации их положений.

Ключевые слова: Таиланд, критическая информационная инфраструктура, безопасность данных, национальная стратегия, информационная безопасность, кибербезопасность, персональные данные, цифровая экономика, электронная торговля, национальная безопасность

Актуальность темы исследования. Последние годы государства Юго-Восточной Азии возглавляют многочисленные рейтинги резкого роста цифровой экономики (digital economy). В своем отчете «e-Conomy SEA Spotlight 2020. At full velocity: Resilient and racing ahead» аналитики Google, Temasek и Bain & Company отметили двукратный рост стоимости цифровой экономики региона в 2019 году по сравнению с 2017 годом (с 50 до 100 млрд долларов США)[1]. Ведущими секторами интернет-экономики выступают 1) электронная торговля (e-Commerce), 2) транспорт и доставка еды, 3) туризм, 4) онлайн-СМИ, 5) финансовые услуги. В 2020 году пандемия внесла коррективы в этот расклад – существенную долю на рынке заняли цифровые продукты и услуги в сфере здравоохранение (HealthTech) и образования (EdTech).

Такие впечатляющие темпы роста цифровой экономики в Юго-Восточной Азии обуславливают необходимость гармонизации законодательства государств-участников Ассоциации государств Юго-Восточной Азии (далее – АСЕАН). Пять участников АСЕАН (Вьетнам, Индонезия, Малайзия, Сингапур, Таиланд) уже присоединились к так называемому Единому окну АСЕАН (ASEAN Single Window) – онлайн-платформе для ускоренного таможенного оформления посредством электронного обмена торговыми документами проведения трансграничных операций. На очереди – гармонизация правил электронной торговли, норм защиты прав потребителей, защиты персональных данных, антимонопольной политики и кибербезопасности, разработка правовой основы разрешения споров в интернете [2]. Среди государств-участников АСЕАН ключевая роль в интеграционных процессах по праву принадлежит Сингапуру. Однако последние годы Таиланд, входящий в двадцатку государств мира, занимающих лидирующие позиции в обеспечении кибербезопасности [3], оспаривает лидерство Сингапура в регионе, выступая с инициативами унификации стандартов информационной безопасности и предлагая свою инфраструктуру и ресурсы для международных проектов. В частности, в 2018 году в Бангкоке совместно с Японией был создан Центр наращивания потенциала кибербезопасности АСЕАН-Япония (ASEAN-Japan Cybersecurity Capacity Building Centre). На его базе происходит 1) проведение тренингов для персонала государственных агентств и органов; 2) повышение квалификации экспертов по кибербезопасности из государств-участников АСЕАН (минимум 280 человек); 3) реализация проекта по привлечению молодежи к решению технических задач кибербезопасности (ASEAN Youth Cybersecurity Technical Challenge) [4].

Наряду с международными инициативами 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). Результаты не заставили долго ждать: только в 2020 году электронная

торговля и транспорт (доставка еды) показали рост на 81% и 42% соответственно [1], а прирост новых пользователей цифровых услуг составил 30%, что в 2020 году показывает общую стоимость интернет-экономики Таиланда в 18 млрд долларов США с прогнозируемым ростом к 2025 году в размере 53 млрд долларов США [5]. Согласно Мировому рейтингу цифровой конкурентоспособности (World Digital Competitiveness Rankings), в котором оценивается преобразование экономик государств мира посредством внедрения цифровых технологий в практику правительства, бизнеса и общества в целом, в 2016 году Таиланд занимал 41 место по уровню цифровизации и 44 место по уровню знаний (для сравнения, в 2020 году он поднялся на 39 и 43 места соответственно [6]).

Поэтому кибербезопасность в Таиланде приобрела первостепенное значение для предприятий и частных лиц, ведь с ростом интернет-экономики растет и количество угроз. Согласно отчету Kaspersky Security Network в 2020 году Таиланд занял 56 место в мире по показателю атак на сервера (более 20 млн инцидентов в 2020 году), 44 место по количеству вредоносного ПО для мобильных устройств, 87 место по общему количеству кибератак (для сравнения: Малайзия - 7-е, Индонезия - 66-е, а Сингапур - 154-е) [7]. Учитывая растущее сотрудничество России с государствами АСЕАН в инвестиционной, энергетической и внешнеполитической сферах, необходимо исследовать национальные инструменты обеспечения информационной безопасности государств региона для выявления положительного опыта и гармонизации общих подходов к процессам. Всё вышесказанное и определяет актуальность исследования.

Цель и задачи исследования. Цель исследования – охарактеризовать нормативно-правовой механизм обеспечения безопасности киберпространства Таиланда. Достижение поставленной цели возможно при последовательном решении следующих задач: определение и характеристика нормативно-правовых инструментов защиты киберпространства; выделение характерных особенностей нормативно-правового механизма обеспечения безопасности киберпространства.

Методология. С целью получения наиболее достоверных научных результатов были использованы системно-структурный, формально-логический и формально-юридический методы.

Предмет исследования, источниковая база исследования. Предмет исследования составляют нормативно-правовые акты Таиланда в сфере обеспечения безопасности киберпространства.

Безопасность Королевства Таиланд рассматривается в научной литературе в двух аспектах. С одной стороны, научный интерес представляет обеспечение национальной безопасности в условиях этноконфессиональных разногласий [8; 9; 10]. С другой стороны, авторы отмечают региональное значение государства как в формате АСЕАН [11; 12; 13], так и в формате Индо-Тихоокеанского региона [14; 15]. Авторы подчеркивают решающее значение Таиланда в формировании военно-политического блока, нацеленного против КНР и России [14, с. 97], а также активную роль этого государства во внешнеполитических процессах в сфере безопасности и борьбы с терроризмом [13]. Информационная безопасность является существенным сектором национальной безопасности, а киберпространство рассматривается многими государствами как часть суверенной территории [16], поэтому представляет научный интерес исследование правового механизма (включающего как нормативно-правовой, так и институциональный)

обеспечения кибербезопасности того или иного государства. В нашем случае мы остановимся на Королевстве Таиланд, имеющего значительный потенциал для Российской Федерации с точки зрения упрочнения позиций в регионе и противостояния антироссийской внешней политике [17, с. 148].

В зарубежной литературе вопросы информационной безопасности Таиланда обсуждаются в аспекте милитаризации киберпространства [18] и усиления цензуры [19]. Исследователи отмечают, что государственная политика в сфере информационной безопасности постепенно приобретает черты, свойственные китайскому государству: жесткая правительственная цензура, создание специальных подразделений для подавления инакомыслия и демократических движений в киберпространстве [20].

Основная часть. В 2007 году был принят Закон Таиланда о компьютерных преступлениях (Computer-Related Crime Act)[21], положивший начало формированию государственного правового механизма информационной безопасности. Принятие и его дальнейшее изменение в 2017 году связывают с попытками правительства, поддерживаемого военной хунтой, установить правовой режим информационного пространства, сходный с китайским – так называемый информационный авторитаризм [22].

В частности, критике поддавались положения закона, устанавливающие ответственность за распространение «ложных или частично ложных», «искаженных или частично искаженных» данных или данных, которые могут «вызвать общественную панику» или нанести вред «поддержанию национальной безопасности, общественной безопасности, национальной экономической безопасности, общественной инфраструктуры, служащей общественным интересам» (ст. 14). Также беспокойство вызвали нормы, дающие полномочия суду решать, какую информацию, признанную ложной и несущей вред третьим лицам и общественности, необходимо удалять из Интернета и компьютерных систем (ст. 16/1, 16/2).

Закон в редакции 2017 года разрешает блокировку и удаление информации, размещенной в Интернете по решению суда на основании запроса комитета по проверке компьютерных данных по причине противоречия общественному порядку или нравственности (ст. 20(3)).

Ужесточение законодательства о компьютерных преступлениях произошло на фоне политических преобразований, запущенных в мае 2014 года после военного переворота, направленных на контроль и влияние на граждан как в реальном, так и виртуальном пространстве. По утверждению исследователей [18; 19], тайское киберпространство стало милитаризованным и глубоко политизированным после переворота: «расширение массового наблюдения и акцент на кибер-наблюдение привели к появлению новой формы цифрового паноптикона, который отличается как по размаху, так и по масштабу от миссии холодной войны» [18, с. 200]. За последние пять лет появились доказательства сбора тайскими вооруженными силами обширной и детальной информации, особенно в беспокойных южных провинциях Паттани, Яла и Наратхиват, где преобладает мусульманское население, сопровождаемое реализацией правительственной политики преднамеренной массовой дезинформации [10; 23]. Поскольку политический аспект информационной безопасности Таиланда не является объектом нашего исследования, рассмотрим какие структурные элементы нормативно-правового характера формируют механизм обеспечения безопасности киберпространства в Таиланде.

Нормативно-правовая основа представлена рядом документом программного и регулирующего характера: это Национальная стратегия кибербезопасности Таиланда 2017–2021, Политика и план национальной безопасности (2019-2022), Закон о компьютерных преступлениях 2007 года (в редакции от 2017 года), Закон о защите персональных данных 2017 года и Закон о кибербезопасности Таиланда 2019 года. Рассмотрим их положения подробнее.

В 2017 году была опубликована Национальная стратегия кибербезопасности Таиланда 2017–2021 (National Cybersecurity Strategy 2017-2021)[24], рассчитанная на применение в течение четырех лет. Это первое руководство по национальной политике Таиланда в сфере кибербезопасности, поставившее целью повышение государства к борьбе с киберугрозами, усиление потенциала в этой области, совершенствование центрального механизма управления национальной кибербезопасностью, а также защиту инфраструктуры, повышение осведомленности во всех секторах и укрепление сотрудничества с зарубежными странами.

Спустя два года после утверждения Национальной стратегии кибербезопасности Таиланда 2017–2021 был принят документ под названием «Политика и план национальной безопасности (2019-2022)» [25]. Пункт 3.3 этого документа перечисляет национальные интересы тайского государства: 3.3.1) независимость, суверенитет и целостность государственных территорий; 3.3.2) стабильность и устойчивость ключевых национальных институтов государства; 3.3.3) безопасность государства и ее жителей от всех видов угроз; 3.3.4) мирное и гармоничное сосуществование, единство и социальная стабильность в плюралистическом обществе, признающем человеческие честь и достоинство; 3.3.5) национальный рост, справедливость, благосостояние и процветание людей; 3.3.6) устойчивость природных ресурсов и окружающей среды, продовольственная и водная безопасность; 3.3.7) способность защищать национальные интересы в изменяющейся международной обстановке; 3.3.8) мирное, благородное и достойное сосуществование с членами АСЕАН и мировым сообществом.

Для обеспечения этих национальных интересов были сформулированы национальные цели (п. 3.4), одной из которых было обозначено продвижение способности и ролей правительства, а также расширение возможности всех секторов в борьбе со всеми типами угроз, влияющих на национальную безопасность (п. 3.4.5). Достижение этой национальной цели осуществляется благодаря сформулированной политике усиления кибербезопасности (Политика №10, п. 3.6.10), объединяющей стратегическую цель, индикаторы и стратегии реализации.

В качестве стратегической цели сформулирован тезис о том, что Таиланд безопасен, защищен и хорошо подготовлен к противодействию киберугрозам. Индикаторов достижения этой цели выделено два: (а) уровень готовности Таиланда к предотвращению кибератак в соответствии с международными принципами; (б) эффективная система кибербезопасности для защиты государственных электронных данных и ключевых кибер-инфраструктур.

Стратегий реализации указанной цели (продвижение способности и ролей правительства, а также расширение возможности всех секторов в борьбе со всеми типами угроз, влияющих на национальную безопасность) определено шесть [25]:

(1) развитие потенциала государственных органов, военных и гражданских агентств, полиции и других акторов для предотвращения и решения проблем безопасности в киберпространстве, в том числе для поддержки цифрового общества;

(2) разработка рамок для международного сотрудничества и сотрудничества стран АСЕАН в предотвращении и противодействие киберугроз;

(3) развитие человеческого капитала, знаний и осведомленности о влиянии киберугроз;

(4) предотвращение киберугроз и устранение любого риска, который может привести к кибервойне, посредством межведомственного управления кибербезопасностью в государственном секторе. Укрепление сетей сотрудничества со всеми субъектами внутри и за пределами Таиланда;

(5) разработка эффективных механизмов обеспечения соблюдения законодательства в сфере кибербезопасности, включая технологии для расследования и предотвращения киберпреступлений;

(6) содействие развитию способности всех организаций и соответствующего персонала приобретать кибер-знания и опыт на постоянной основе.

Подводя промежуточный итог, можно говорить о всеобъемлющем характере «Политики и плана национальной безопасности (2019-2022)» как программного документа, охватывающего направления внешней и внутренней политики и всех заинтересованных субъектов.

Возвращаясь к Национальной стратегии кибербезопасности 2017-2021, реализация которой завершается в этом году, отметим девять задач, выполнение которых будет свидетельствовать об ее успешной реализации: а) повышение доверия в каждом секторе к реализации всех форм кибер-деятельности; б) защита информационной инфраструктуры, управляемой информационными системами, и развитие возможности для борьбы с киберугрозами; в) защита национальных интересов и национальной безопасности от старых и новых угроз; г) укрепление цифровой экономики; д) повышение интеграции и сотрудничества, включая обмен информацией о кибербезопасности между институциональными элементами системы информационной безопасности; е) развитие потенциала агентств и увеличение возможностей сотрудников в сфере кибербезопасности; ж) продвижение культуры ответственного использования киберпространства; з) содействие работе по предупреждению и пресечению преступности; и) повышение международной роли Таиланда в поддержании безопасности [24].

Стратегия определяет пять направлений, по которым осуществляется постоянная оценка готовности к киберугрозам:

(1) готовность нормативно-правовой базы – правовые меры по обеспечению кибербезопасности можно разделить на три группы. Первую группу формируют положения Закона об электронной торговле, который устанавливает ключевые меры безопасности для снижения рисков и обеспечения надежности при использовании информационных систем для электронных транзакций, включая государственные электронные услуги и работу электронного правительства. Ко второй группе относятся нормы, регулирующие надзор за финансово-банковским сектором со стороны Банка Таиланда и Управления Комиссии по ценным бумагам и биржа. И третья группа представлена нормами Закона о компьютерных преступлениях.

(2) готовность оперативных подразделений по борьбе с киберугрозами. Специальные подразделения создаются как в государственном секторе – в Королевской полиции Таиланда, Министерстве юстиции, Министерстве обороны, Департаменте по борьбе с

отмыванием денег, Банке Таиланда и т.д., так и в частном секторе – так называемые CERT (computer emergency response team, группа реагирования на компьютерные чрезвычайные ситуации) - ThaiCERT, например). Подчеркивается необходимость развития механизма координации и взаимодействия таких подразделений, а также системы аудита их деятельности.

(3) готовность персонала. Опрос, проведенный в организациях государственного и частного секторов, показал, что более 50% респондентов не придают значения повышению квалификации персонала в сфере кибербезопасности, а 79% респондентов имеют ограничения в такой мотивации. Поэтому необходимо пересмотреть политику повышения квалификации, сделав упор на обучение на международно-сертифицированных курсах.

(4) готовность систем и технологий. Таиланд пока зависит от зарубежных производителей информационных технологий и устройств, поэтому подчеркивается необходимость поддержки национальных производителей и развития системы сертификации/стандартизации импортируемого оборудования.

(5) готовность к расследованию инцидентов и кибер-разведке. В настоящее время существуют проблемы с интеграцией и развитием потенциала кибер-разведки, которая играет важную роль в понимании новых типов угроз, в частности киберугроз. Поэтому необходимо усовершенствовать методики расследований киберинцидентов и методики анализа данных.

Авторы стратегии определили семь факторов (проблем и тенденций), учет которых необходимо осуществлять в течение четырех лет ее реализации.

Первый фактор – это проблема неправильного выбора приоритетов пользователями товаров и услуг в интернет-пространстве. В качестве основного приоритета выбирается удобство, а безопасность стоит на втором-третьем (после стоимости).

Второй фактор – это проблема уязвимость к определенным типам кибератак. Наиболее распространенные – это malware-атаки, ransomware-атаки и DoS/DDoS-атаки на объекты критически информационной инфраструктуры (электроэнергетика, водоснабжение, газоснабжение, коммунальные службы и т. д.

Третий фактор – это глобализация мировых финансовых рынков. Появление новых финансовых инструментов (мобильные финансовые приложения, краудфандинг, финансовые платформы (маркетплейсы) и т. д.) демонстрирует слабую готовность правительств к их регулированию. Поэтому пересмотр нормативных актов должен быть оперативным и учитывать специфику финансово-банковского сектора (доверительный характер деятельности, уязвимость персональных данных, страхование рисков, резкое качественное и количественное увеличение объема транзакций и т. д.).

Четвертый фактор – проблема недооценки государственными агентствами тренингов по кибербезопасности (учитывающих ситуации до атаки, во время и после атаки).

Пятый фактор – проблема кибертерроризма и риск вовлеченности в кибервойну. Подчеркивается, что Таиланд может стать объектом террористических атак со стороны государств, террористических организаций и отдельных лиц. Интернет может быть как орудием кибертеррористов (интернет-СМИ, например), так и инструментом распространения идеологии использования насилия или обучения терроризму, равно как и средством распространения оружия и боеприпасов, вербовки членов

экстремистских/террористических организаций. В связи с этим государство должно определять группы риска, развивать свой потенциал по противостоянию информационным атакам и обеспечивать национальную безопасность с учетом этого нового типа угрозы.

Шестой фактор – проблема недостаточной осведомленности о киберугрозах при использовании Интернета. Как отмечалось выше, многие пользователи Интернета ставят безопасность на второе место после удобства в качестве основного приоритета. Поэтому важно повышать осведомленность широкой общественности и пользователей Интернета об угрозах, существующих в киберпространстве, и о средствах защиты от кибератак.

Седьмым фактором выступают риски киберугрозы. Киберугрозы проявляются во многих формах, например, в повреждении систем, краже данных в компьютерных системах (коммерческие, финансовые или персональные данные), а также в атаках на критическую информационную инфраструктуру, что может привести к нарушению функционирования экономической системы и причинить ущерб или подвергнуть опасности жизнь и имущество населения. Киберугрозы постоянно совершенствуются по мере развития технологий: обнаруживаются новые уязвимости в операционных системах, приложениях или программном обеспечении устройств IoT (Internet of things, интернет вещей).

Национальная стратегия кибербезопасности 2017-2021 сопровождается двумя приложениями в форме таблиц. Первая таблица показывает взаимосвязи национальных миссий, политик, стратегий и генеральных планов с Национальной стратегией кибербезопасности на 2017–2021 годы. К таким документам относится, в частности, Проект Национальной стратегии безопасности на 20 лет (2017–2036), статья 5 которого предусматривает разработку механизмов международного сотрудничества на всех уровнях; предотвращение и устранение транснациональных угроз; снижение воздействия терроризма и улучшение информационных технологий и кибербезопасности; разработка эффективной системы разведки. Упоминается уже рассмотренная выше Национальная политика и план национальной безопасности (2017–2021), Национальный план экономического и социального развития №12, а также План цифрового развития экономики и общества.

Вторая таблица, прилагаемая к стратегии, раскрывает подробный оперативный план ее реализации по каждому из направлений: (1) стимулирование всех секторов к разным видам киберактивности; (2) защита критически важной информационной инфраструктуры и разработка потенциальных ответов на киберугрозы; (3) защита национальных интересов от новых и старых киберугроз; (4) укрепление цифровой экономики; (5) повышение осведомленности и продвижение внутреннего сотрудничества при обеспечении кибербезопасности; (6) поощрение культуры использования киберпространства в правильном направлении; (7) содействие работе по профилактике и борьбе с преступностью; (8) продвижение инициатив Таиланда в сфере кибербезопасности на региональном и международном уровне [24].

Подводя промежуточный итог, отметим непростую ситуацию, в которой оказался Таиланд при реализации рассматриваемой стратегии: нежелание зависеть от технологий США, КНР и России ввиду нестабильных политических отношений определило обращение тайского правительства к частным разработчикам информационных технологий, в частности к итальянской компании Hacking Team, специализирующийся на средствах взлома и слежки (это было подтверждено фактом набора офицеров в 2015 году для работы в новом подразделении Cyber Warfare при Управлении совместных операций

Королевских вооруженных сил Таиланда) [26]. Основным продуктом Hacking Team является система дистанционного управления «Галилео». Пакет программного обеспечения Hacking Team был приобретен Королевской армией Таиланда и Департаментом исправительных учреждений Королевской полиции Таиланда в сотрудничестве с израильской компанией Nice Systems и партнерскими тайскими фирмами Placing Value, Netsurplus и Samart Comtech. Он включает функции тайного сбора электронных писем, текстовых сообщений и историй телефонных звонков; ведения журнала нажатий клавиш; открытия данных истории поиска; записи аудио с телефонных разговоров; использования телефонов для сбора шума и разговоров путем удаленного включения телефона; активирования камеры телефона и т.д. Хотя противники режима осуждают использование такого программного обеспечения правительственными органами ввиду отсутствия демократических институтов контроля [20], на наш взгляд, ситуацию необходимо оценивать с нескольких позиций: национальной безопасности, борьбы с террористической угрозой, обеспечения государственного строя и прав и свобод человека. Очевидно, что ограничение последних допустимо в свете роста экстремистских и террористических движений в государстве.

Регулирование отношений в киберпространстве осуществляется на основе нескольких законов. Одним из них является Закон о компьютерных преступлениях 2007 года (в редакции от 2017 года) [21], состоящий из двух частей (parts): первая посвящена описанию составов компьютерных преступлений и санкций за их совершение (статьи 5-17/1), а вторая – полномочиям компетентных органов по их расследованию (статьи 18-31). Закон содержит глоссарий, в котором раскрываются такие понятия, как «компьютерная система», «компьютерные данные», «данные трафика», «поставщик услуг», «пользователь» и др. Компетентным государственным органом, уполномоченным исполнять данный закон, является созданное в 2017 году Министерство цифровой экономики и общества Таиланда. На него возложены полномочия по установлению стандартов кибербезопасности, включая наблюдение и поддержание безопасности информационных телекоммуникаций Королевства Таиланд. Привлечение к ответственности за совершение правонарушений согласно рассматриваемому закону осуществляется Комитетом по штрафам (Fine Committee). К компьютерным преступлениям (правонарушениям) относятся такие действия как 1) незаконный доступ к компьютерной системе (ст. 5); 2) незаконный доступ к компьютерным данным (ст. 7); 3) незаконные операции с компьютерными данными, принадлежащие другому лицу (ст. 9); 4) рассылка спама без возможности отписаться от респондента (ст. 11); 5) размещение ложных компьютерных данных в компьютерной системе, могущее нанести ущерб третьей стороне или общественности (ст. 14) и другие. В качестве мер наказания закон предусматривает лишение свободы и штрафы до 400 тыс. тайских бат.

Уголовный кодекс Королевства Таиланд 1956 года (в редакции 2019 года) [27] содержит четыре статьи устанавливающих ответственность за совершение преступлений в информационном пространстве: а) подделка документов (ст. 264); б) использование чужих платежных карт (статьи 269/1-269/7); в) мошенничество (ст. 341); г) злоупотребление доверием (ст. 342 (1)).

Закон о защите персональных данных (Personal Data Protection Act, далее - PDPA) [28] был разработан и принят в сжатые сроки после вступления в силу Общего регламента по защите данных ЕС (General Data Protection Regulation, далее - GDPR). Принятие этого закона было вызвано необходимостью согласования правового режима площадок электронной торговли Таиланда с общеевропейским режимом конфиденциальности

данных. PDPA заимствует ряд положений из GDPR.

Во-первых, это определение ключевых терминов (ст. 6): персональные данные (информация, которая может прямо или косвенно идентифицировать личность, за исключением информации об умершем человеке и данных частного бизнеса, таких как контактная информация, должности или адреса); контроллер данных (физическое или юридическое лицо, которое имеет право принимать решения о сборе, использовании или раскрытии персональных данных); обработчик данных (физическое или юридическое лицо, которое собирает, использует или раскрывает персональные данные в соответствии с распоряжениями контроллера данных).

Во-вторых, это строгие требования к конфиденциальности при сборе, хранении и обработке так называемых «чувствительных» персональных данных (ст. 26) о расовом или этническом происхождении, политических взглядах, религиозных или философских убеждениях, судимости, членстве в профсоюзах, генетические данных, биометрических данных, медицинских данных, сексуальной ориентации или предпочтениях. Сбор таких персональных данных без явного согласия владельца данных запрещен, за исключением определенных обстоятельств, таких как неотложная медицинская помощь или в соответствии с требованиями закона.

В-третьих, права владельца данных (ст. 30-42) в соответствии с PDPA аналогичны правам в GDPR. В частности, владельцы данных имеют право запрашивать доступ к своим персональным данным и возможность отправлять запросы на удаление, уничтожение или анонимность своих данных.

В-четвертых, это необходимость получения четкого и явного согласия (в письменной форме или через электронную систему) на сбор персональных данных (ст. 19), такие запросы не должны вводить субъекта в заблуждение. Владельцы данных могут отозвать свое согласие в любое время, но отзыв не может повлиять на предыдущий сбор, использование или раскрытие персональных данных, которые были разрешены законом. Исключения из требований согласия довольно широки и охватывают договорные обязательства, общественные интересы и законные основания.

И наконец, как и в случае с европейским регламентом, тайский PDPA предусматривает создание специального органа, уполномоченного на разработку рекомендаций по соблюдению положений этого акта (глава I) – Комитет по защите персональных данных (Personal Data Protection Committee).

PDPA состоит из шести глав, посвященных регулированию таких вопросов, как правовой статус Комитета по защите персональных данных (глава I), защита персональных данных (глава II), права субъекта данных (глава III), правовой статус администрации Комитета по защите персональных данных (глава IV), жалобы (глава V), гражданско-правовая ответственность (глава VI), штрафы (уголовная ответственность, административная ответственность) (глава VII). В качестве наказаний предусмотрены лишение свободы (до 1 года) и штрафы (до пяти млн тайских бат).

28 мая 2019 года в силу вступил Закон о кибербезопасности Таиланда 2019 года (далее – Закон) [29]. Закон был принят с целью управления, содействия и реагирования на быстрорастущую цифровую экономику государства. Он регулирует надзор за деятельностью в области кибербезопасности, а также предотвращение и борьбу с «киберугрозами», которые в широком смысле определяются как «любые действия или незаконные действия, совершаемые с использованием компьютера, компьютерной системы или нежелательной программы с намерением причинить вред кому-либо,

компьютерной системе, компьютерным данным или другим соответствующим данным, а также непосредственные угрозы, которые могут вызвать повреждение или повлиять на работу компьютера, компьютерной системы или других соответствующих данных» (ст. 3).

Одной из особенностей данного Закона является указание в преамбуле тезиса об ограничении прав и свобод человека, гарантированных Конституцией Королевства Таиланд, с целью «эффективной защиты кибербезопасности и разработки подходов для защиты, преодоления и снижения риска киберугроз, влияющих на национальную безопасность и общественный порядок. Принятие этого Закона соответствует критериям, установленным в статье 26 Конституции Королевства Таиланд» [29].

Закон состоит из четырех глав (chapters). Глава 1 регламентирует правовой статус Комитета (Committee), состоящего из Национального комитета кибербезопасности (National Cybersecurity Committee, NCSC) и Комитета по регулированию кибербезопасности (Cybersecurity Regulating Committee). Глава 2 посвящена регулированию деятельности Администрации Национального комитета кибербезопасности (Office of the National Cybersecurity Committee), глава 3 – системе поддержания кибербезопасности (Maintaining Cybersecurity), включающей политики и планы (policies and plans), управление (management), критическую информационную инфраструктуру (critical information infrastructure) и противодействие киберугрозам (coping with cyber threats). Последняя глава содержит положения о наказаниях (penalty provisions).

В статье 3 дается определение терминов, используемых в Законе. В частности, «поддержание кибербезопасности» (Maintaining Cybersecurity) означает любую меру или процедуру, установленную для предотвращения, преодоления и снижения риска киберугроз как внутри страны, так и за ее пределами, которые влияют на национальную безопасность, экономическую безопасность, военную безопасность и общественный порядок в стране. «Инцидент кибербезопасности» (Cybersecurity Incident) означает инцидент, вызванный любым действием или незаконным обязательством, совершенным через компьютер или компьютерную систему, которое может повредить или повлиять на кибербезопасность или кибербезопасность компьютера, компьютерных данных, компьютерной системы или других данных, связанных с компьютерной системой.

«Решение кибербезопасности» (Cybersecurity Solution) означает акт решения проблемы кибербезопасности с использованием персонала, процессов и технологий через компьютер, компьютерную систему, компьютерную программу или любую услугу, относящуюся к компьютеру, для создания уверенности и повышения кибербезопасности компьютера, компьютерных данных, компьютерной системы или других данных, относящихся к компьютерной системе.

Представляет интерес определение терминов, имеющих отношение к критической информационной инфраструктуре (далее - КИИ) – ключевому объекту кибербезопасности. Тайский закон определяет ее как компьютер или компьютерную систему, которую правительственное агентство или частная организация использует в своих операциях, связанных с поддержанием национальной безопасности, общественной безопасности, национальной экономической безопасности или инфраструктуры в общественных интересах. Отметим, что вместо термина «оператор КИИ», используемого в России, КНР и других странах [30; 31], Закон оперирует термином «организация критически важной информационной инфраструктуры» (Organization of Critical Information Infrastructure), в качестве которой может рассматриваться правительственное агентство или частная организация, которая ответственна за

предоставление услуг КИИ или оказывает эти услуги непосредственно. Контроль и регулирование деятельности организации КИИ осуществляется «надзорной или регулирующей организацией» (Supervising or Regulating Organization) – то есть правительственным агентством или частной организацией или лицом, которые уполномочены законом.

Как мы отмечали ранее [30; 31], критическая информационная инфраструктура – основной объект кибератак злоумышленников и основной объект информационной безопасности государства, от сохранности и стабильного функционирования которой зависит благополучие каждого человека, общества и государства в целом. Поэтому рассмотрим, какой правовой режим КИИ установил тайский законодатель в 2019 году.

Статья 48 Закона отмечает, что КИИ важна для национальной безопасности, военной безопасности, экономической безопасности и общественного порядка в стране. В ст. 49 дается перечень секторов КИИ, к которым отнесены: (1) национальная безопасность; (2) государственная служба; (3) банковское дело и финансы; (4) информационные технологии и телекоммуникации; (5) транспорт и логистика; (6) энергетика и коммунальные услуги; (7) общественное здравоохранение; (8) другие сектора, определенные Комитетом.

В качестве организации КИИ Комитет самостоятельно определяет конкретную организацию, которая обязана в установленные сроки (30 дней) предоставить необходимую информацию (ст. 52).

Надзорная или регулирующая организация проводит проверку организации КИИ установленным стандартам кибербезопасности (ст. 53), а также проводит оценку рисков (ст. 54). Все предписания должны быть выполнены в установленные сроки (ст. 53, 55).

На организации КИИ возлагаются определенные обязательства: (i) предоставление собственником/владельцем необходимой информации для учета уполномоченными государственными органами; (ii) соблюдение сводов правил и минимальных стандартов кибербезопасности; (iii) организация оценки риска кибербезопасности не реже одного раза в год (результаты такой оценки должны представляться уполномоченным государственным органам); (iv) внедрение механизмов или процедур мониторинга и устранения любых киберугроз или инцидентов, связанных с организацией КИИ; и (v) сообщение о любых киберугрозах.

Часть 4 главы 3 посвящена противодействию киберугрозам (coping with cyber threats). Как указывалось выше, Комитет уполномочен определять три уровня киберугроз: (1) несерьезные киберугрозы (non-serious cyber threats); (2) серьезные киберугрозы (serious cyber threats); (3) критические киберугрозы (critical cyber threats). Характеристика каждого уровня угрозы зависит, среди прочего, от воздействия такой угрозы на государственную инфраструктуру, национальную безопасность, экономику, общественное здравоохранение и общество. Предпринимаемые меры определяются уровнем опасности: например, в случае серьезной киберугрозы уполномоченные органы имеют право проверять компьютеры, компьютерные системы и кибер-данные, а также изымать компьютеры, компьютерные системы или любое другое оборудование.

Последняя глава Закона содержит нормы, устанавливающие уголовные санкции за совершение преступлений в сфере кибербезопасности (ст. 70-77). В частности, уголовному преследованию подвергаются [29]:

1) должностные лица, нарушающие конфиденциальность любых данных (лишение

свободы на срок до трех лет и (или) штраф до 60 тыс. бат (ст. 70-72));

2) организации КИИ за сокрытие информации о киберинциденте (штраф до 200 тыс. бат (ст. 73)) или любой другой информации (штраф до 100 тыс. бат (ст. 74));

3) любые лица, нарушающее или не выполняющее распоряжения Комитета (в зависимости от вида нарушения - общий штраф до 300 тыс. бат и штраф за каждый день невыполнения распоряжения до 10 тыс. бат; лишение свободы на срок до одного года и (или) штраф до 20 тыс. бат (ст. 75); лишение свободы до трех лет и (или) штраф до 60 тыс. бат (ст. 76)).

Выводы. В результате проведенного исследования мы пришли к следующим выводам. Нормативно-правовой механизм обеспечения безопасности киберпространства Таиланда представлен программными и регулирующими документами: Национальная стратегия кибербезопасности Таиланда 2017–2021, Политика и план национальной безопасности (2019-2022), Закон о компьютерных преступлениях 2007 года (в редакции от 2017 года), Уголовный кодекс 1956 года (в редакции 2019 года), Закон о защите персональных данных 2017 года и Закон о кибербезопасности 2019 года. Первые два документа содержат задачи и индикаторы их решения для достижения ключевой цели кибербезопасности. В отличие от КНР [16, с. 118] и России [32] Таиланд в своих стратегических документах не определяет основные информационные угрозы во внутренней и внешней сфере, а также приоритеты развития системы кибербезопасности. Напротив, как и Сингапур [33, с. 111], Таиланд очерчивает круг национальных интересов и ставит задачи, выполнение которых способно вывести его в лидеры региона. Законы разработаны с учетом последних тенденций в сфере информационных технологий и включают в сферу регулирования такие вопросы как защита персональных данных, компьютерных и информационных систем, критически важной информационной инфраструктуры. Законодательно установлена вертикаль государственного управления и мониторинга, очерчен круг полномочий компетентных органов. В сфере защиты персональных данных законодательство Таиланда в значительной мере дублирует положения Общего регламента по защите данных Евросоюза. Отличительной чертой нормативно-правовых актов является легальное обоснование ограничения прав и свобод человека при реализации их положений.

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. e-Conomy SEA Spotlight 2020. At full velocity: Resilient and racing ahead // Google e-Conomy SEA 2020, URL: https://economysea.withgoogle.com/#explore.
2. Iwamoto K. Rise of digital economy pushes ASEAN toward policy coordination / K. Iwamoto // NIKKEI: Asian Review, URL: https://asia.nikkei.com/Politics/Rise-of-digital-economy-pushes-ASEAN-toward-policy-coordination2.
3. Toomgum S. Thailand among top 20 nations focusing on cybersecurity / S. Toomgum // The Nation, URL: http://www.nationmultimedia.com/detail/Economy/30325029.
4. ASEAN-Japan Cybersecurity Capacity Building Centre (Step 2) // Japan-ASEAN cooperation, URL: https://jaif.asean.org/support/project-brief/asean-japan-cybersecurity-capacity-building-centre.html.

5. e-Conomy SEA Spotlight 2020. At full velocity: Resilient and racing ahead. Country Insights: Thailand // Google e-Conomy SEA 2020, URL: https://storage.googleapis.com/gweb-economy-sea.appspot.com/assets/pdf/Thailand-e-Conomy_SEA_2020_Country_Insights.pdf.
6. IMD World Digital Competitiveness Ranking 2020 // IMD World Competitiveness Center, URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/
7. Fight to foil cyberthreats intensifies // Bangkok Post, URL: https://www.bangkokpost.com/business/2105531/fight-to-foil-cyberthreats-intensifies.
8. Зайцев В.О. Этноконфессиональные проблемы Таиланда и пути их решения / В.О. Зайцев // Инновации. Наука. Образование. 2020. № 24. С. 1803-1810.
9. Фомичева Е.А. Причины и типологические особенности публичных протестов в Таиланде в 2020 г. / Е.А. Фомичева // Юго-Восточная Азия: актуальные проблемы развития. 2020. Т. 3. № 3 (48). С. 156-166.
10. Рогожина Н.Г. Проблема глубокого юга Таиланда-сепаратизм малайских мусульман / Н.Г. Рогожина // Контуры глобальных трансформаций: политика, экономика, право. 2021. Т. 14. № 1. С. 176-193.
11. Пылева А.И. Взаимоотношения Франции и Королевства Таиланд в общем контексте региональной безопасности Юго-восточной Азии / А.И. Пылева // Актуальные проблемы региональной безопасности современной Азии и Африки.-Санкт-Петербург, 2013. С. 535-557.
12. Лобач Д.В. Современные террористические угрозы в Юго-восточной Азии / Д.В. Лобач // Азиатско-тихоокеанский регион: экономика, политика, право. 2017. Т. 19. № 2-3. С. 153-172.
13. Сомкамнерд Н. Особенности региональной политики Таиланда в региональных процессах Юго-восточной Азии / Н. Сомкамнерд // Вопросы национальных и федеративных отношений. 2018. Т. 8. № 2 (41). С. 170-179.
14. Райков Ю.А. Фактор АСЕАН в политике США в восточной Азии / Ю.А. Райков // США и Канада: экономика, политика, культура. 2020. Т. 50. № 2. С. 97-113.
15. Срисанит В. Всеобъемлющее региональное экономическое партнерство: возможности и вызовы для Таиланда / В. Срисанит // Юго-Восточная Азия: актуальные проблемы развития. 2020. Т. 3. № 4 (49). С. 132-144.
16. Горян Э.В. Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики / Э.В. Горян // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2021. Т. 13. № 1. С. 115–124.
17. Батюк В.И. Индо-тихоокеанская стратегия США и Евразия / В.И. Батюк // Актуальные проблемы Европы. 2021. № 1 (109). С. 135-153.
18. Pinkaew L. Mass surveillance and the militarization of cyberspace in post-coup Thailand / L. Pinkaew // ASEAS-Austrian Journal of South-East Asian Studies. 2016. №9(2). – Pp. 195-214.
19. Schaffar W. New social media and politics in Thailand: The emergence of fascist vigilante groups on Facebook / W. Schaffar // ASEAS – Austrian Journal of South-East Asian Studies. 2016. №9(2). – Pp. 215-234.
20. McDermott G. Thailand's Creeping Digital Authoritarianism / G. McDermott // The Diplomat, URL: https://thediplomat.com/2021/02/thailands-creeping-digital-authoritarianism/.
21. Computer-Related Crime Act, B.E. 2550 (2007) // Ministry of Digital Economy and

Society, URL: https://www.mdes.go.th/law/detail/3618-COMPUTER-RELATED-CRIME-ACT-B-E--2550--2007-.

22. Thailand: Cyber Crime Act Tightens Internet Control // Human Rights Watch, URL: https://www.hrw.org/news/2016/12/21/thailand-cyber-crime-act-tightens-internet-control.
23. Cogan M.S. The age of government (dis)information in Thailand / M.S. Cogan // Globe Media Asia, URL: https://southeastasiaglobe.com/thailands-disinformation-age/.
24. National Cybersecurity Strategy 2017-2021 // Council of Europe, URL: https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/thailand?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/.
25. The National Security Policy and Plan (2019-2022) // Office of the National Security Council, URL: http://www.nsc.go.th/wp-content/uploads/2020/05/The-National-Security-Policy-and-Plan2019-–-2022.pdf.
26. Draper J. Thailand acquires advanced electronic surveillance police state capability / J. Draper // Prachatai, URL: https://prachatai.com/english/node/5345.
27. Criminal Code, B.E. 2499 (1956) // Thailand Law Omline, URL: https://www.thailandlawonline.com/laws-in-thailand/thailand-criminal-law-text-translation#269.
28. Personal Data Protection Act, B.E. 2562 (2019) // Thai Netizen, URL: https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf
29. Cybersecurity Act, B.E. 2562 (2019) // Office of the Council of State, URL: http://web.krisdika.go.th/data/document/ext843/843708_0001.pdf.
30. Горян Э.В. Идентификация объектов критической информационной инфраструктуры в Российской Федерации и Сингапуре: сравнительно-правовой аспект / Э.В. Горян // Административное и муниципальное право. 2018. № 11. С.44-56.
31. Горян Э.В. Критическая информационная инфраструктура Китайской Народной Республики: особенности правового регулирования в аспекте обеспечения информационной безопасности финансово-банковского сектора / Э.В. Горян // Административное и муниципальное право. 2020. № 4. С. 45-57.
32. Концепция стратегии кибербезопасности Российской Федерации. – Текст: электронный // Совет Федерации Федерального Собрания Российской Федерации: [сайт]. – 2014. – URL: http://council.gov.ru/services/discussions/themes/38324/.
33. Горян Э.В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения / Э.В. Горян // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103–117

Результаты процедуры рецензирования статьи

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

на статью
Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве Таиланда

Название отчасти соответствует содержанию материалов статьи.
В названии статьи условно просматривается научная проблема, на решение которой направлено исследование автора.
Рецензируемая статья представляет относительный научный интерес. Автор разъяснил выбор темы исследования и обосновал её актуальность.
В статье, на взгляд рецензента, не вполне корректно сформулирована цель исследования, указан его предмет и перечислен ряд методов, использованных автором. Основные элементы «программы» исследования автором не вполне продуманы, что отразилось на его результатах. В названии статьи автор заявил о намерении изучить «нормативно-правовую основу обеспечения национальной безопасности в киберпространстве Таиланда», однако в тексте пообещал «охарактеризовать национальную стратегию кибербезопасности Таиланда и выделить положения, детерминирующие потенциал международного сотрудничества с Россией». Почему автор ограничил «нормативно-правовые основы» одним документом и почему сместил внимание на международное сотрудничество России, он не разъяснил.
Автор не представил результатов анализа историографии проблемы, ограничившись заявлением о том, что его «поиск в электронной библиотеке научных публикаций eLIBRARY.RU показал отсутствие научных исследований рассматриваемой темы». При этом автор сделал вывод, что «такой недостаток научных публикаций доказывает необходимость исследования данной темы». Автор не сформулировал новизну предпринятого исследования, что является существенным недостатком статьи.
Апелляция к оппонентам в статье отсутствует.
Автор избирательно опирался на источники и актуальные научные труды по теме исследования.
Автор не разъяснил выбор и не охарактеризовал круг источников, привлеченных им для раскрытия темы.
Автор разъяснил и обосновал выбор географических рамок исследования.
На взгляд рецензента, автор стремился грамотно использовать источники, выдержать научный стиль изложения, грамотно использовать методы научного познания, соблюсти принципы логичности, систематичности и последовательности изложения материала.
В качестве вступления автор указал на причину выбора темы исследования, обосновал её актуальность, сформулировал цель и предмет исследования, перечислил методы. Автор обратил внимание читателя на то, что в государствах Юго-Восточной Азии происходит «резкий рост цифровой экономики (digital economy)» т.д., что «впечатляющие темпы роста» «обуславливают необходимость гармонизации законодательства государств-участников Ассоциации государств Юго-Восточной Азии» и что Таиланд претендует на роль нового лидера «в обеспечении кибербезопасности», «выступая с инициативами унификации стандартов информационной безопасности и предлагая свою инфраструктуру и ресурсы для международных проектов» т.д. При этом автор заключил, что «исследовать национальные инструменты обеспечения информационной безопасности государств региона для выявления положительного опыта и гармонизации общих подходов к процессам», необходимо, «учитывая растущее сотрудничество России с государствами АСЕАН» т.д.
В основной части статьи автор сообщил, что в 2017 году в Тайландк приняли «Национальную стратегию кибербезопасности», указал цели, на которые направлено принятие данного документа, сообщил, что в 2019 г. был утверждён другой законодательный акт – «Политика и план национальной безопасности (2019-2022)», в котором были сформулированы соответствующие «национальные интересы тайского государства» и национальные цели «для обеспечения этих национальных интересов».

Далее, следуя содержанию документа, автор назвал два индикатора достижения «стратегической цели» в области обеспечения кибербезопасности и 6 «стратегий реализации». Читателю необходимо самостоятельно понять, «стратегии реализации» чего имел в виду автор: «Национальной стратегии кибербезопасности» или «Политики и плана национальной безопасности (2019-2022)». Мысль сформулирована неясно. Как соотносятся между собой два данных документа по назначению, автор читателю не разъяснил.

Схожим образом автор перечислил 9 задач, путём которых возможно «достижение цели Национальной стратегии кибербезопасности 2017-2021», затем кратко описал содержание 5 направлений, по которым осуществляется «постоянная оценка готовности к киберугрозам» («готовность нормативно-правовой базы» т.д., «готовность оперативных подразделений по борьбе с киберугрозами» т.д., «готовность персонала» т.д., «готовность систем и технологий» т.д., «готовность к расследованию инцидентов и кибер-разведке» т.д.), перечислил «семь факторов (проблем и тенденций), учет которых необходимо осуществлять» в процессе реализации, видимо, «Национальной стратегии кибербезопасности».

В завершение основной части статьи автор сообщил место Тайланда в Мировом рейтинге цифровой конкурентоспособности 2016 и 2020 гг. и констатировал «удовлетворительный уровень подготовки государства к киберугрозам» т.д. Неожиданно автор заявил, что «рассматриваемый документ сопровождается двумя приложениями в форме таблиц» и кратко описал их содержание».

Выводы не позволяют оценить научные достижения автора в рамках проведенного им исследования. Выводы не отражают результатов исследования, проведённого автором, в полном объёме.

В заключительном абзаце статьи автор констатировал, что «Таиланд в своих стратегических документах не определяет основные информационные угрозы во внутренней и внешней сфере, а также приоритеты развития системы кибербезопасности» т.д., что особенностью его «национальной стратегии является отсутствие терминологического глоссария». Совершенно внезапно автор сообщил, что «с точки зрения потенциала сотрудничества с Российской Федерацией, положения стратегии подчеркивают необходимость международного взаимодействия и не ограничивают круг возможных партнеров» т.д.

Заключительный абзац статьи не проясняет цель исследования.

На взгляд рецензента, потенциальная цель исследования достигнута автором отчасти.

Публикация потенциально может вызвать интерес у аудитории журнала.

Статья требует существенной доработки, начиная с формулирования ключевых элементов программы исследования, заканчивая соответствующими им выводами.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ

на статью на тему «Нормативно-правовой механизм обеспечения безопасности киберпространства Таиланда».

Предмет исследования.

Предложенная на рецензирование статья посвящена актуальным вопросам правового регулирования отношений по поводу обеспечения безопасности киберпространства

Таиланда. Рассматриваются проблемы толкования законодательства, а также различные материалы практики. В качестве предмета исследования автором заявлены «нормативно-правовые акты Таиланда в сфере обеспечения безопасности киберпространства». Помимо этого, автором изучается научная литература по вопросам, заявленным в рамках статьи, а также некоторые эмпирические данные (например, статистика).

Методология исследования.

Цель исследования прямо заявлена в статье. «Цель исследования – охарактеризовать нормативно-правовой механизм обеспечения безопасности киберпространства Таиланда. Достижение поставленной цели возможно при последовательном решении следующих задач: определение и характеристика нормативно-правовых инструментов защиты киберпространства; выделение характерных особенностей нормативно-правового механизма обеспечения безопасности киберпространства». Исходя из поставленных цели и задач, автором выбрана методологическая основа исследования.

В частности, автором используется совокупность общенаучных методов познания: анализ, синтез, аналогия, дедукция, индукция, другие. В частности, методы анализа и синтеза позволили обобщить и разделить выводы различных научных подходов к предложенной тематике, а также сделать конкретные выводы из эмпирических материалов.

Наибольшую роль сыграли специально-юридические методы. В частности, автором активно применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства Таиланда (прежде всего, положений актов по поводу обеспечения безопасности киберпространства). Например, следующие рассуждения автора: «В частности, критике поддавались положения закона, устанавливающие ответственность за распространение «ложных или частично ложных», «искаженных или частично искаженных» данных или данных, которые могут «вызвать общественную панику» или нанести вред «поддержанию национальной безопасности, общественной безопасности, национальной экономической безопасности, общественной инфраструктуры, служащей общественным интересам» (ст. 14). Также беспокойство вызвали нормы, дающие полномочия суду решать, какую информацию, признанную ложной и несущей вред третьим лицам и общественности, необходимо удалять из Интернета и компьютерных систем (ст. 16/1, 16/2)».

Также автором для иллюстрации своих выводов используются материалы практики, в том числе статистические данные. В частности, отмечается следующее: «Наряду с международными инициативами 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). Результаты не заставили долго ждать: только в 2020 году электронная торговля и транспорт (доставка еды) показали рост на 81% и 42% соответственно [1], а прирост новых пользователей цифровых услуг составил 30%, что в 2020 году показывает общую стоимость интернет-экономики Таиланда в 18 млрд долларов США с прогнозируемым ростом к 2025 году в размере 53 млрд долларов США [5]. Согласно Мировому рейтингу цифровой конкурентоспособности (World Digital Competitiveness Rankings), в котором оценивается преобразование экономик государств мира посредством внедрения цифровых технологий в практику правительства, бизнеса и общества в целом, в 2016 году Таиланд занимал 41 место по уровню цифровизации и 44 место по уровню знаний (для сравнения, в 2020 году он поднялся на 39 и 43 места соответственно [6])».

Таким образом, в целом выбранная автором методология в полной мере адекватна цели исследования, позволяет изучить все аспекты темы в ее совокупности.

Актуальность.

Актуальность заявленной проблематики не вызывает сомнений. Имеется как теоретический, так и практический аспекты значимости предложенной темы. С точки зрения теории проблема установления механизмов регулирования безопасности киберпространства очень сложна и требует глубокого осмысления учеными разных стран. Использование опыта разных стран способно предложить различные механизмы формирования наиболее эффективных подходов к кибербезопасности. С позиции практики анализ и толкование нормативно-правовых актов Таиланда может быть использован специалистами и деятелями в сфере международной торговли. Автор прав в том, что страны Юго-Восточной Азии все больше становятся вовлеченными в международную торговую деятельность, все больше становятся в центре внимания крупных организаций. Не секрет, что сейчас нередко бизнес ведется через интернет. Следовательно, участникам таких отношений следует внимательно относится к законодательству Таиланда, в том числе в сфере обеспечения безопасности в киберпространстве.

Тем самым, научные изыскания в предложенной области стоит только поприветствовать.

Научная новизна.

Научная новизна предложенной статьи не вызывает сомнений. Во-первых, она выражается в конкретных выводах автора. Среди них, например, такой вывод:

«Нормативно-правовой механизм обеспечения безопасности киберпространства Таиланда представлен программными и регулирующими документами: Национальная стратегия кибербезопасности Таиланда 2017–2021, Политика и план национальной безопасности (2019-2022), Закон о компьютерных преступлениях 2007 года (в редакции от 2017 года), Уголовный кодекс 1956 года (в редакции 2019 года), Закон о защите персональных данных 2017 года и Закон о кибербезопасности 2019 года. Первые два документа содержат задачи и индикаторы их решения для достижения ключевой цели кибербезопасности. В отличие от КНР [16, с. 118] и России [32] Таиланд в своих стратегических документах не определяет основные информационные угрозы во внутренней и внешней сфере, а также приоритеты развития системы кибербезопасности. Напротив, как и Сингапур [33, с. 111], Таиланд очерчивает круг национальных интересов и ставит задачи, выполнение которых способно вывести его в лидеры региона. Законы разработаны с учетом последних тенденций в сфере информационных технологий и включают в сферу регулирования такие вопросы как защита персональных данных, компьютерных и информационных систем, критически важной информационной инфраструктуры. Законодательно установлена вертикаль государственного управления и мониторинга, очерчен круг полномочий компетентных органов. В сфере защиты персональных данных законодательство Таиланда в значительной мере дублирует положения Общего регламента по защите данных Евросоюза. Отличительной чертой нормативно-правовых актов является легальное обоснование ограничения прав и свобод человека при реализации их положений».

Указанный и иные теоретические выводы могут быть использованы в дальнейших научных исследованиях.

Во-вторых, автором оригинальные обобщения нормативно-правового материалы Таиланда. Кроме того, автором дано толкование использованных норм и положений законодательства. В том числе, приведенные выводы могут быть актуальны и полезны для правотворческой деятельности в процессе совершенствования законодательства

других стран и России.
Таким образом, материалы статьи могут иметь определенных интерес для научного сообщества с точки зрения развития вклада в развитие науки.

Стиль, структура, содержание.
Тематика статьи соответствует специализации журнала «Вопросы безопасности», так как она посвящена правовым проблемам, связанным с безопасностью в киберпространстве с позиции компаративистского подхода.
Содержание статьи в полной мере соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели исследования.
Качество представления исследования и его результатов следует признать в полной мере положительным. Из текста статьи прямо следуют предмет, задачи, методология и основные результаты исследования.
Оформление работы в целом соответствует требованиям, предъявляемым к подобного рода работам. Существенных нарушений данных требований не обнаружено.

Библиография.
Следует высоко оценить качество использованной литературы. Автором активно использована литература, представленная авторами из России и из-за рубежа (Горян Э.В., Райков Ю.А., Батюк В.И., Пылева А.И., Рогожина Н.Г., Schaffar W., McDermott G. Cogan M.S., Draper J. и другие). Многие из цитируемых ученых являются признанными учеными в области заявленных автором проблем. Хотело бы отметить использование автором большого количества нормативно-правовых актов Таиланда.
Таким образом, труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию различных аспектов темы.

Апелляция к оппонентам.
Автор провел серьезный анализ текущего состояния исследуемой проблемы. Все цитаты ученых сопровождаются авторскими комментариями. То есть автор показывает разные точки зрения на проблему и пытается аргументировать более правильную по его мнению.

Выводы, интерес читательской аудитории.
Выводы в полной мере являются логичными, так как они получены с использованием общепризнанной методологии. Статья может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к вопросам применения нормативно-правовых актов Таиланда в сфере обеспечения безопасности в киберпространстве.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи
«Рекомендую опубликовать»