Научная статья

УДК 341.171

DOI https://doi.org/10.24866/VVSU/2073-3984/2021-3/108-116

Э.В. Горян

Владивостокский государственный университет экономики и сервиса
Владивосток. Россия

Информационная безопасность в киберпространстве: опыт правового регулирования Таиланда*

Объектом исследования являются отношения, возникающие при обеспечении информационной безопасности в киберпространстве. Характеризуются положения Национальной стратегии кибербезопасности и Закона о кибербезопасности Таиланда как ключевых документов, определяющих систему гарантий информационной безопасности. С целью получения наиболее достоверных научных результатов использованы системно-структурный, формально-логический и формально-юридический методы. Закон о кибербезопасности 2019 года устанавливает эффективный механизм обеспечения информационной безопасности в киберпространстве как в институциональном аспекте, так и нормативно-правовом. В первом случае создана вертикаль государственного управления и мониторинга, во втором – определены секторы КИИ и минимальные требования к организациям КИИ. Отличительной чертой рассматриваемого закона является нормативное обоснование ограничения прав и свобод человека при реализации его положений, а также установление уголовных санкций за совершение преступлений должностными лицами как государственных органов, так и частных компаний. Такие санкции выступают в качестве дополнительной гарантии прав и свобод человека в сфере информации и персональных данных.

Ключевые слова и словосочетания: кибербезопасность, национальный механизм, Таиланд.

Горян Элла Владимировна – канд. юрид. наук, доцент, доцент кафедры гражданско-правовых дисциплин; e-mail: ella.goryan@vvsu.ru

* *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».*

E.V. Gorian

Vladivostok State University of Economics and Service
Vladivostok. Russia

Informational security in cyberspace: the legal regulation outcomes of Thailand

The provisions of the Thailand's National Cybersecurity Strategy 2017-2021 and the Cybersecurity Act 2019 being the key documents defining the system of information security guarantees are characterized. To obtain the most reliable scientific results, the system-structural, formal-logical and formal-legal methods were used. The Cybersecurity Act 2019 establishes an effective mechanism for ensuring information security in cyberspace, both in institutional and regulatory aspects. In the former, a vertical of public administration and monitoring was created, in the latter, the sectors of the CII and the minimum requirements for the organizations of the CII were determined. A distinctive feature of the act is the regulatory justification for the restriction of human rights and freedoms in the implementation of its provisions, as well as the imposition of criminal sanctions for the crimes of state officials and private companies officers. Such sanctions act as an additional guarantee of human rights concerning personal data and freedom of information.

Keywords: cybersecurity, national mechanism, Thailand.

Актуальность темы исследования

Последние годы государства Юго-Восточной Азии возглавляют многочисленные рейтинги в связи с резким ростом цифровой экономики (digital economy). Эксперты отмечают двукратный рост стоимости цифровой экономики региона в 2019 году по сравнению с 2017 годом (с 50 до 100 млрд долларов США) [5]. 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 здравоохранения (HealthTech) и образования (EdTech). Это способствует повышению внимания национальных регуляторов к информационной безопасности как на уровне государства, так и на уровне региона. Государства, стремящиеся занять лидирующие позиции в регионе, строят свою внешнюю и внутреннюю политику с учетом этого фактора. Например, Таиланд, входящий в двадцатку государств мира, занимающих лидирующие позиции в обеспечении кибербезопасности [9], оспаривает лидерство Сингапура, 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) [3]. Наряду с международными инициативами Таиланд проводит активное наращивание нормативно-правовой базы для регулирования процессов кибербезопасности. В течение трех лет с 2017 по 2019 год были приняты Национальная страте-

гия 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 [5], 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 [6].

Кибербезопасность в Таиланде приобрела первостепенное значение для предприятий и частных лиц, ведь с ростом интернет-экономики увеличивается и количество угроз. Согласно отчету Kaspersky Security Network, в 2020 году Таиланд занял 56 место в мире по показателю атак на серверы (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, Индонезия – 66, а Сингапур – 154) [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 исследования – охарактеризовать нормативно-правовую основу информационной безопасности в киберпространстве Таиланда и выделить ее особенности.

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

Предмет исследования составляют положения Национальной стратегии кибербезопасности Таиланда 2017–2021 и Закона о кибербезопасности Таиланда 2019 года.

Поиск в электронной библиотеке научных публикаций eLIBRARY.RU показал отсутствие научных исследований по рассматриваемой теме. Немногочисленные статьи посвящены общим аспектам безопасности в Юго-Восточной Азии. Такой недостаток научных публикаций доказывает необходимость исследования данной темы.

Основная часть. В 2017 году была опубликована Национальная стратегия кибербезопасности Таиланда 2017–2021 (National Cybersecurity Strategy 2017–2021) [8], рассчитанная на применение в течение четырех лет. Это первое руководство по национальной политике Таиланда в сфере кибербезопасности, поставившее целью повышение роли государства в 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.

Достижение цели Национальной стратегии кибербезопасности 2017–2021 возможно путем решения девяти задач: 1) повышение доверия в каждом секторе к реализации всех форм кибердеятельности; 2) защита информационной инфраструктуры, управляемой информационными системами, и развитие возможности для борьбы с киберугрозами; 3) защита национальных интересов и национальной безопасности от старых и новых угроз; 4) укрепление цифровой экономики; 5) повышение интеграции и сотрудничества, включая обмен информацией о кибербезопасности между институциональными элементами системы информационной безопасности; 6) развитие потенциала агентств и увеличение возможностей сотрудников в сфере кибербезопасности; 7) продвижение культуры ответственного использования киберпространства; 8) содействие работе по предупреждению и пресечению преступности; 9) повышение международной роли Таиланда в поддержании безопасности [8].

Рассматриваемый документ 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, вторая 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 уровнях.

28 мая 2019 года в силу вступил Закон о кибербезопасности Таиланда 2019 года (далее – Закон) [4], который 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» [4, 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» [4].

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 cyberthreats). 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, экономическую, 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, который может повредить или повлиять на безопасность в целом–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 используют в своих операциях, связанных с поддержанием национальной, общественной, национальной экономической безопасности или инфраструктуры в общественных интересах. Отметим, что вместо термина «оператор КИИ», используемого в России, КНР и других странах [1; 2], Закон оперирует термином «организация критически важной информационной инфраструктуры» (Organization of Critical Information Infrastructure), в качестве которой могут рассматриваться правительственное агентство или частная организация, ответственная за предоставление услуг КИИ или оказывающая эти услуги непосредственно. Контроль и регулирование деятельности организации КИИ осуществляются «надзорной или регулирующей организацией» (Supervising or Regulating Organization), то есть правительственным агентством, частной организацией или лицом, которые уполномочены законом.

Национальный комитет кибербезопасности (National Cybersecurity Committee, NCSC, далее – Комитет) формируется из следующих должностных лиц: 1) премьер-министр в качестве председателя; 2) директора по должности (directors by position): министр обороны, министр цифровой экономики и общества, постоянный секретарь Министерства финансов, постоянный секретарь Министерства юстиции, генеральный комиссар Национального полицейского управления и генеральный секретарь Совета национальной безопасности; 3) почетные директора в количестве не более семи человек, назначаемых Кабинетом министров из лиц, обладающих знаниями, опытом и значительным опытом в области обеспечения кибербезопасности, информационных технологий и коммуникаций, защиты конфиденциальности данных, науки, техники, права, финансов или других соответствующих аспектов (ст. 5).

Комитет имеет следующие обязанности и полномочия (ст. 9): 1) предлагать политику и план по поддержанию кибербезопасности; 2) определять политику управления для поддержания кибербезопасности государственных агентств и организаций КИИ; 3) готовить оперативный план по поддержанию кибербезопасности для рассмотрения Кабинетом министров; 4) устанавливать стандарты и руководства для улучшения и развития систем обслуживания, относящихся к поддержанию кибербезопасности, устанавливать стандарты в отношении компьютерной техники, компьютерных систем, компьютерных программ, а также утверждать стандарты сертификации организаций КИИ, государственных агентств, надзорных или регулирующих организаций, частных организаций; 5) разрабатывать меры и руководящие принципы для повышения уровня знаний и опыта компетентных должностных лиц, включая должностных лиц организации КИИ и иных субъектов; 6) устанавливать пределы сотрудничества с другими национальными и зарубежными агентствами в сфере кибербезопасности; 7) отслеживать и оценивать результаты работы в соответствии с политикой, общим и оперативным планами по поддержанию кибербезопасности; 8) предоставлять заключения Комитету по цифровой экономике и обществу (the Digital Economy and Society Committee) или Кабинету министров по вопросам обеспечения кибербезопасности; 9) выступать с законодательной инициативой в сфере кибербезопасности и т.д.

Для выполнения обязанностей и полномочий Комитета в соответствии со ст. 9 создается Комитет по регулированию кибербезопасности (Cybersecurity Regulating Committee), в состав которого входят: 1) министр цифровой экономики и общества в качестве председателя; 2) директора по должности, включая постоянного секретаря Министерства иностранных дел, постоянного секретаря Министерства транспорта, постоянного секретаря Министерства цифровой экономики и общества, постоянного секретаря Министерства энергетики, постоянного секретаря Министерства внутренних дел, постоянного секретаря Министерства здравоохранения, генерального комиссара Национального полицейского управления, Верховного главнокомандующего, генерального секретаря Совета национальной безопасности, директора Национального разведывательного управления, управляющего Банка Таиланд, генерального секретаря Комиссии

по ценным бумагам и биржам и Генерального секретаря Национальной комиссии по телерадиовещанию и электросвязи; 3) почетные директора в количестве четырех человек, назначаемых Комитетом из числа лиц, обладающих знаниями и опытом, которые важны и полезны для поддержания кибербезопасности (ст. 12).

Комитет по регулированию кибербезопасности имеет следующие обязанности и полномочия: 1) контроль за выполнением плана по поддержанию кибербезопасности, утвержденному согласно ст. 9(1) и ст. 42; 2) отслеживание и принятие мер для противодействия киберугрозам на критическом уровне; 3) регулирование деятельности национальных координирующих агентств по безопасности компьютерных систем, реагированию на инциденты и компьютерной криминалистике; 4) регулирование деятельности организации КИИ; 5) мониторинг уровня киберугроз, включая подробную информацию о мерах по предотвращению, противодействию, оценке на каждом уровне с последующим предоставлением отчета Национальному комитету кибербезопасности.

При разработке стандартов деятельности организаций КИИ должны быть рассмотрены принципы управления рисками, содержащие, как минимум, следующие подходы и меры: описание риска, который может возникнуть в отношении компьютера, компьютерных данных, компьютерной системы, другой информации, связанной с компьютерной системой, имуществом, жизнью и здоровьем человека; меры по предотвращению риска; меры по изучению и мониторингу киберугроз; меры реагирования при обнаружении киберугроз; меры по устранению и восстановлению ущерба, причиненного киберугрозой.

Как мы отмечали ранее [1; 2], 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 статье 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 секторы, 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 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 упол-

номоченными 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 предоставляться уполномоченным государственным органам); (iv) внедрение механизмов или процедур мониторинга и устранения любых киберугроз или инцидентов, связанных с организацией КИИ; (v) сообщение о любых киберугрозах.

Часть 4 главы 3 посвящена противодействию киберугрозам (coping with cyberthreats). Как указывалось выше, Комитет уполномочен определять три уровня киберугроз: 1) несерьезные киберугрозы (non-serious cyberthreats); 2) серьезные киберугрозы (serious cyberthreats); 3) критические киберугрозы (critical cyberthreats). Характеристика каждого уровня угрозы зависит от воздействия такой угрозы на государственную инфраструктуру, национальную безопасность, экономику, общественное здравоохранение и общество. Предпринимаемые меры определяются уровнем опасности: в случае серьезной киберугрозы уполномоченные органы имеют право проверять компьютеры, компьютерные системы и киберданные, 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 [4]:

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, нарушающие или не выполняющие 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 выводам, что Закон о кибербезопасности 2019 года устанавливает эффективный механизм обеспечения информационной безопасности в киберпространстве как в институциональном аспекте, так и нормативно-правовом. В первом случае создана вертикаль государственного управления и мониторинга, во втором – определены секторы КИИ и минимальные требования к организациям КИИ. Отличительными чертами рассматриваемого закона являются нормативное обоснование ограничения прав и свобод человека при реализации его положений, а также установление уголовных санкций за совершение преступлений должностными лицами как государственных органов, так и частных компаний. Такие санкции выступают в качестве дополнительной гарантии прав и свобод человека в сфере информации и персональных данных.

1. Горян Э. В. Идентификация объектов критической информационной инфраструктуры в Российской Федерации и Сингапуре: сравнительно-правовой аспект // Административное и муниципальное право. – 2018. – № 11. – С. 44–56.

2. Горян Э. В. Критическая информационная инфраструктура Китайской Народной Республики: особенности правового регулирования в аспекте обеспечения информационной безопасности финансово-банковского сектора // Административное и муниципальное право. – 2020. – № 4. – С. 45–57.
3. ASEAN-Japan Cybersecurity Capacity Building Centre (Step 2). – Текст: электронный // Japan-ASEAN cooperation: [сайт]. – URL: https://jaif.asean.org/support/project-brief/asean-japan-cybersecurity-capacity-building-centre.html (дата обращения: 15.08.2021).
4. Cybersecurity Act, B.E. 2562 (2019). – Текст: электронный // Office of the Council of State: [сайт]. – URL: http://web.krisdika.go.th/data/document/ext843/843708_0001.pdf (дата обращения: 15.08.2021).
5. e-Conomy SEA Spotlight 2020. At full velocity: Resilient and racing ahead. – Текст: электронный // Google e-Conomy SEA 2020: [сайт]. – URL: https://economysea.withgoogle.com/#explore (дата обращения: 15.08.2021).
6. e-Conomy SEA Spotlight 2020. At full velocity: Resilient and racing ahead. Country Insights: Thailand. – Текст: электронный // Google e-Conomy SEA 2020: [сайт]. – URL: https://storage.googleapis.com/gweb-economy-sea.appspot.com/assets/pdf/Thailand-e-Conomy_SEA_2020_Country_Insights.pdf (дата обращения: 15.08.2021).
7. Fight to foil cyberthreats intensifies. – Текст: электронный // Bangkok Post: [сайт]. – URL: https://www.bangkokpost.com/business/2105531/fight-to-foil-cyberthreats-intensifies (дата обращения: 15.08.2021).
8. National Cybersecurity Strategy 2017-2021. – Текст: электронный // Council of Europe: [сайт]. – URL: https://www.coe.int/en/web/octopus/country-wiki-ap/ /asset_publisher/CmDb7M4RGb4Z/content/thailand?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/ (дата обращения: 15.08.2021).
9. Toomgum S. Thailand among top 20 nations focusing on cybersecurity. – Текст: электронный // The Nation: [сайт]. – URL: http://www.nationmultimedia.com/detail/Economy/30325029 (дата обращения: 15.08.2021).

References

1. Goryan E. V. Identifikaciya ob"ektov kriticheskoj informacionnoj infrastruktury v Rossijskoj Federacii i Singapure: sravnitel'no-pravovoj aspekt // Administrativnoe i municipal'noe pravo. – 2018. – № 11. – S. 44–56.
2. Goryan E. V. Kriticheskaya informacionnaya infrastruktura Kitajskoj Narodnoj Respubliki: osobennosti pravovogo regulirovaniya v aspekte obespecheniya informacionnoj bezopasnosti finansovo-bankovskogo sektora // Administrativnoe i municipal'noe pravo. – 2020. – № 4. – S. 45–57.

© Э.В. Горян, 2021

Для цитирования: Горян Э.В. Информационная безопасность в киберпространстве: опыт правового регулирования Таиланда // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2021. – Т. 13, № 3. – С. 108–116.

For citation: Gorian E.V. Informational security in cyberspace: the legal regulation outcomes of Thailand, *The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2021, Vol. 13, № 3, pp. 108–116.

DOI https://doi.org/10.24866/VVSU/2073-3984/2021-3/108-116

Дата поступления: 17.08.2021.