Национальная безопасность / nota bene
Правильная ссылка на статью:
Горян Э.В. — Роль финансового регулятора Таиланда в обеспечении информационной безопасности финансово-банковского сектора // Национальная безопасность / nota bene. – 2022. – № 5. DOI: 10.7256/2454-0668.2022.5.39079 EDN: HTPVVG URL: https://nbpublish.com/library_read_article.php?id=39079

Роль финансового регулятора Таиланда в обеспечении информационной безопасности финансово-банковского сектора

Горян Элла Владимировна

ORCID: 0000-0002-5962-3929

кандидат юридических наук

доцент, Владивостокский государственный университет

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

ella-gorjan@yandex.ru

Статья из рубрики "Управление и обеспечение систем безопасности"

DOI:

10.7256/2454-0668.2022.5.39079

EDN:

HTPVVG

Дата направления статьи в редакцию:

26-10-2022

Дата публикации:

02-11-2022

Аннотация: Объектом исследования являются отношения, возникающие при функционировании национального правового механизма обеспечения кибербезопасности. Предмет исследования представлен нормативно-правовыми актами и источниками «мягкого права» Таиланда, устанавливающими требования к информационным системам субъектов финансово-банковского сектора. На примере второй экономики в Юго-Восточной Азии – Таиланде, определяется роль финансового регулятора государства – Банка Таиланда (Bank of Thailand, BOT) в обеспечении кибербезопасности финансового и банковского секторов. Выделяются особенности правового статуса Банка Таиланда, детерминирующие координационную роль в институциональном механизме обеспечения кибербезопасности. Исследуются ключевые документы финансового регулятора, формирующие нормативно-правовой механизм обеспечения кибербезопасности Таиланда. Полномочия финансового регулятора Таиланда распределены между тремя органами. Банк Таиланда контролирует

коммерческие банки, финансовые компании, кредитные учреждения, компании по управлению активами, услуги электронных платежей и компании, выпускающие кредитные карты. Комиссия по ценным бумагам и биржевым операциям осуществляет надзор за операциями с ценными бумагами, в то время как Комиссия по страхованию - надзор за деятельностью страховых компаний. Обеспечение информационной безопасности возложено на Банк Таиланда, уполномоченного на создание системы управления рисками финансовых учреждений в целях обеспечения их стабильности. С этой целью он принимает нормативные акты, устанавливающие стандарты безопасности трех видов информационных систем: общего характера, обслуживающих электронные платежи и обслуживающих электронные платежные карты. Заслуживает внимания требование к операторам информационных систем при заключении соглашения об обслуживании определить права внутренних и внешних аудиторов, а также должностное лицо Банка Таиланда для проверки операций и контроля поставщика услуг. Финансовый регулятор определяет статус поставщиков услуг особо важных платежных систем, вменяя им в обязанность разрабатывать меры безопасности информационных систем в зависимости от типов и сложности их собственных услуг.

Ключевые слова:

финансово-банковский сектор, информационная безопасность, финансовый регулятор, цифровая инфраструктура, критическая информационная инфраструктура, Таиланд, финтех, оператор информационной системы, информационная система, цифровые технологии

Актуальность. Атаки на компьютерные системы осуществляются в отношении наиболее важных для общества и государства секторов: энергетический, транспортный, финансовый, банковский и проч. Такие информационные системы имеют статус критических информационных инфраструктур и находятся под постоянным наблюдением специализированных институтов, уполномоченных государством на обеспечение их информационной безопасности. Но усилий одних таких институтов недостаточно, они обеспечивают всего лишь неприкосновенность и бесперебойное функционирование компьютерных систем, однако иные вопросы безопасности (например, конфиденциальность данных) остаются под ответственностью субъектов, которые используют эти системы. Особое место среди таких субъектов занимают финансовые институты, доверие к которым и зависит от обеспечения конфиденциальности и гарантийных обязательств. Координирующую роль в финансовом и банковском секторе играет финансовый регулятор, устанавливающий правила осуществления деятельности финансовыми институтами, в том числе в сфере обеспечения безопасности их функционирования. Чем более и значительным для международной экономики является государство, тем более серьезные атаки совершаются на его финансовые институты. Таиланд является второй экономикой Юго-восточной Азии, оспаривая своё лидерство в регионе с Сингапуром и осуществляя ряд мер по усилению инвестиционной привлекательности субъектов финансово-банковского сектора. Фактором притока инвестиций в этот сектор является информационная безопасность, поскольку современная экономика имеет цифровой характер. Поэтому Таиланд наращивает своё присутствие на международной арене, выступая в качестве надежного партнера в деле обеспечения международной безопасности. В частности, в 2018 году в Бангкоке совместно с Японией был создан Центр наращивания потенциала кибербезопасности АСЕАН-Япония (ASEAN-Japan CybersecurityCapacity 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 YouthCybersecurityTechnical Challenge) (ASEAN-Japan CybersecurityCapacity Building Centre (Step 2), URL: https://jaif.asean.org/support/project-brief/asean-japan-cybersecurity-capacity-building-centre.html).

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) иЗакон 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, а в пандемийный 2020 год прирост составил 12%. Прирост новых пользователей цифровых услуг составил 30%, что в 2021 году показывает общую стоимость интернет-экономики Таиланда в 35 млрд. долларов США с прогнозируемым ростом к 2025 году в размере 53 млрд. долларов США (e-Conomy SEA Spotlight 2022. Through the waves, towards a sea of opportunity, URL: https://economysea.withgoogle.com/#explore).

Поэтому изучение опыта Таиланда по обеспечению кибербезопасности вообще [1; 2] и деятельности его финансового регулятора в рассматриваемой сфере в частности необходимо для совершенствования российского механизма кибербезопасности. Все вышесказанное свидетельствует об актуальности темы исследования.

Цель исследования - охарактеризовать роль финансового регулятора Таиланда – Банка Таиланда (Bank of Thailand), в обеспечении информационной безопасности финансово-банковского сектора. Задачи исследования заключаются в определении правового статуса финансового регулятора, его функций и характере сотрудничества с частным сектором в указанной сфере.

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

Предмет исследования, источниковая база исследования, противоречия в имеющихся исследованиях и авторская позиция. Предмет исследования представлен нормативно-правовыми актами и источниками «мягкого права» Таиланда, устанавливающими требования к информационным системам субъектов финансово-банковского сектора.

Выбранная нами для исследования тема мало представлена в российской научной литературе. Следует отметить, что отечественные научные исследования о роли российского финансового регулятора в обеспечении информационной безопасности банковской и финансовой систем публикуются регулярно, но компаративистические исследования в указанной сфере практически отсутствуют. Упоминание о зарубежном опыте участия финансовых регуляторов в механизме обеспечения кибербезопасности можно найти в работах И.И. Аминова [3], В.В. Масленникова [4], Н.С. Молодцова [5] и А.К. Трифоновой [6]. Деятельности финансовых регуляторов Сингапура, Китая и Россиив рассматриваемой сфере был посвящен ряд наших исследований [7; 8; 9] 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».

Основная часть. Полномочия финансового регулятора Таиланда распределены между тремя органами. Банк Таиланда (Bank of Thailand, BOT) контролирует коммерческие банки, финансовые компании, кредитные учреждения, компании по управлению активами, услуги электронных платежей и компании, выпускающие кредитные карты. Комиссия по ценным бумагам и биржевым операциям (The Securities and Exchange Commission, SEC) осуществляет надзор за операциями с ценными бумагами. Комиссия по страхованию (Office of Insurance Commission, OIC) осуществляет надзор за деятельностью страховых компаний.

Банк Таиланда был первоначально создан как Национальное банковское бюро Таиланда. Закон о Банке Таиланда был обнародован 28 апреля 1942 года, возлагая на Банк Таиланда ответственность за все функции центрального банка. Банк Таиланда начал свою деятельность 10 декабря 1942 года. Позже в Закон о Банке Таиланда были внесены поправки, чтобы подчеркнуть его социальную ответственность, создать механизм защиты от экономического кризиса, а также настроить процесс принятия решений для обеспечения надлежащего управления и прозрачности в организации. В настоящее время действует редакция Закона о Банке Таиланда от 2008 года (Bank of Thailand Act B.E.2485 as amended by B.E.2551, URL: https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/Documents/LAW01_BOTAct.pdf

В соответствии с этим законом, Банк Таиланда имеет следующую компетенцию:

1)печать и выпуск банкнот и других ценных бумаг; 2) содействие денежно-кредитной стабильности и разработка денежно-кредитной политики; 3) управление активами Банка Таиланда;4) предоставление банковских услуг правительству и регистрация государственных облигаций; 5) предоставление банковских услуг финансовым учреждениям; 6) создание или поддержка создания платежной системы; 7) контроль и аудит финансовых учреждений путем изучения и анализа финансового состояния и деятельности, а также создания системы управления рисками финансовых учреждений в целях обеспечения их стабильности; 8) управление курсом иностранной валюты в рамках валютной системы и управление активами в валютном резерве в соответствии с Законом о валюте (Currency Act B.E. 2501, URL: https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/Documents/LAW02_CurrencyAct 9) валютный контроль.

Нормативно-правовую базу деятельности Банка Таиланда составляют следующие законы и подзаконные нормативные акты. Закон о Банке Таиланда устанавливает цели, объем работы и организационную структуру Банка Таиланда в соответствии с международным стандартом центрального банка для поддержания стабильности и эффективности финансовой системы, системы финансовых учреждений и платежной системы за счет прозрачных и подотчетных процедур.

В соответствии с Законом о валюте Банк Таиланда обязан управлять международными резервами и поддерживать валютный резерв в соответствии с соответствующими законами для обеспечения стабильности и доверия к валюте. Кроме того, финансовый регулятор также обязан разрабатывать, печатать, выпускать, управлять и контролировать банкноты, чтобы обеспечить наличие банкнот в достаточном количестве в обращении в соответствии со спросом экономической системы.

Закон о валютном контроле (Exchange Control Act B.E. 2485, URL:

https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/Documents/LAW03_ExchangeCo содержит принципы контроля, ограничения или запрета на осуществление всех обменных или других операций с иностранной валютой в любой форме.

Закон о платежной системе (Payment System Act B.E 2560 (2017), URL: https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/Documents/LAW04_PaymentSys направлен на осуществление надзора за работой платежных систем и платежных услуг в целях обеспечения стабильности, безопасности и эффективности платежных систем в целом и в соответствии с международными стандартами, включая поддержку платежных инноваций. Закон определяет три вида платежных систем: важнейшая платежная система (Highly Important Payment System), назначенная платежная система (Designated Payment System) и назначенная платежная служба (Designated Payment Service), в отношении которых Банк Таиланда имеет право осуществлять надзор. Любое лицо, желающее управлять платежной системой или платежной службой, указанной в Уведомлении министра финансов в качестве назначенной платежной системы или назначенной платежной службы, должно получить лицензию у министра финансов или зарегистрироваться в Банке Таиланда.

Закон о предпринимательской деятельности финансовых учреждений (Financial Institution Business Act B.E. 2551 (2008), URL: https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/Documents/LAW05_FIAct.pdf) регулирует меры по управлению рисками финансовых учреждений, обеспечение регулирования банковской деятельности и защиты от ущерба, который может возникнуть в результате деятельности финансовых учреждений. Он также имеет целью поддержание экономической стабильности и доверия вкладчиков и общественности, устанавливая правила надлежащего управления для любого лица, выполняющего обязанности директора, менеджера, должностного лица или лица, наделенного полномочиями по управлению финансовыми учреждениями.

Чрезвычайное постановление о компании по управлению активами (Emergency Decree on Asset Management Companies, B.E.2541 (1998), URL: https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/Documents/LAW06_AMCAct.pdf определяет механизм регистрации компании по управлению активами, которая будет получать преимущества в виде освобождения от уплаты сборов и налогов при покупке или получении неработающих активов или их залога от финансовых учреждений. Кроме того, Банк Таиланда имеет право осуществлять надзор за компанией по управлению активами в соответствии с полномочиями, указанными в этом чрезвычайном постановлении.

Закон о коммерческой деятельности в сфере кредитной информации (Credit Information Business Operation Act, B.E. 2545 (2002), URL: https://www.bot.or.th/English/AboutBOT/LawsAndRegulations/Documents/LAW07_NCBAct.pdf требует достаточной информации о финансовом состоянии и истории платежей своих клиентов, т. е. о том, какова история клиентов и сколько долгов у клиентов перед другими финансовыми учреждениями. В прошлом у финансовых учреждений не было такой информации; таким образом, это способствовало увеличению просроченных кредитов и проблем для финансовых учреждений и системы финансовых учреждений в целом.

Комиссия по ценным бумагам и биржевым операциям (The Securities and Exchange Commission, URL: https://www.sec.or.th/EN/Pages/ABOUTUS/HOWWEREGULATE.aspx контролирует и регулирует рынки капитала в соответствии с законодательством о ценных

бумагах и биржевых операциях, деривативах, цифровых активах, доверительном управлении для сделок на рынке капитала, юридических лицах специального назначения для целей секьюритизации, резервном фонде.

Цели деятельности по администрированию положений и правил: 1) обеспечение доступа инвесторов к информации и принятию решений об инвестициях; 2) эффективная, прозрачная и честная работа рынка капитала; 3) контроль и сдерживание в определенных пределах систематических рисков на рынках.

Комиссия по страхованию (Office of Insurance Commission, OIC) является регулятором страховой отрасли Таиланда, работающим под руководством министра финансов Таиланда. Комиссия уполномочена регулировать деятельность страховых компаний, брокеров и агентов и была создана в соответствии с Законом о государственной страховой комиссии Таиланда (Government Insurance Commission Act, B.E. 2550, URL: https://www.oic.or.th/sites/default/files/content/91311/insurance-commission-act-be-2007.pdf), в котором функции Комиссии определялись как «надзор и содействие ведению страхового бизнеса». Комиссия отвечает за выдачу операционных лицензий для страховых компаний и операционное соблюдение правил посредством надзора за рынком.

Банк Таиланда разработал комплекс инструментов, с помощью которых осуществляется обеспечение информационной безопасности субъектов финансово-банковского сектора. Это так называемые уведомления (notifications), устанавливающие: 1) нормы осуществления операций с электронными платежными картами; 2) политику и меры по обеспечению безопасности информационной системы для коммерческой деятельности поставщиков услуг электронных платежей (вместе с Руководством по безопасности информационной системы, относящейся к услуге электронных платежей); 3) политику и меры по безопасности систем информационных технологий (вместе с Руководством по безопасности информационных систем, связанных с платежными системами).

Осуществление операций с электронными платежными картами устанавливается уведомлением Банка Таиланд о правилах, процедурах и условиях ведения бизнеса с электронными платежными картами (Notification of the Bank of Thailand No. FPG. 6/2559 Re: Rules, Procedures and Conditions for Undertaking Electronic Money Card Business, URL: https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/EngPDF/25610093.pdf&sa=U&ved=2aB2dFpctUsb). Финансовый регулятор устанавливает ответственность поставщика услуг за непрерывность, безопасность и надежность услуг. Поставщик услуг должен осуществлять надлежащее управление рисками при выборе поставщиков услуг и соответствующие процедуры мониторинга, оценки и надзора за услугами назначенных поставщиков услуг. Кроме того, поставщик услуг должен заключить со своими контрагентами соглашение об обслуживании, в котором определяются права внутренних и внешних аудиторов, а также должностного лица Банка Таиланда на проверку операций и внутреннего контроля поставщика услуг.

Поставщик услуг должен реализовывать политику безопасности в отношении своих услуг, которая включает в себя управление доступом к системе и данным, аутентификацию клиентов и неотказуемость, целостность системы и данных, конфиденциальность данных, доступность системы, мониторинг системы, а также отчет о происшествиях в случае нарушения работы системы в течение более чем 24 часов. На него возлагается обязанность не реже одного раза в год проверять и оценивать свои информационные системы в соответствии с политикой и мерами по безопасности информационной системы, установленными Банком Таиланда; и представить копию

отчета о проверке в Банк Таиланда в течение 30 дней со дня завершения проверки.

Политика и меры по обеспечению безопасности информационных систем поставщиков услуг электронных платежей (вместе с Руководством по безопасности информационных систем поставщиков услуг электронных платежей) устанавливаются соответствующим уведомлением Банка Таиланда (The Bank of Thailand Notification No. ITG. 3/2552 Re: Policies and Measures on Security of Information System for Business Operation of Electronic Payment Service Providers, URL: https://www.bot.or.th/English/PaymentSystems/Payment_Regulation/BN_Regulation/BAHTNET 2560_2017-05-26_ISO_BN_ICAS_EN%2520(2).pdf&sa=U&ved=2ahUKEwjN0M7_por7AhWH6aQKHb6TCpQQFnc В соответствии с этим документом поставщики услуг должны соответствовать стандартам, политике и мерам по безопасности информационной системы. Поставщики услуг должны ознакомить своих сотрудников с одобренной высшим руководством политикой безопасности информационной системы, а также проводить обучение персонала и регулярно проводить обзор или корректировку политики в соответствии с текущей ситуацией (п. 4.1). Такая политика должна включать положения о а) контроле доступа и аутентификации; б) конфиденциальности информации и целостности системы; в) доступности системы; г) экспертизе безопасности информационной системы.

Поставщики услуг должны разработать комплекс мер по обеспечению безопасности информационных систем (п. 4.2). Такие меры должны соответствовать характеристикам бизнеса и включать контроль доступа и аутентификацию, конфиденциальность информации, целостность информационной системы, доступность системы, реагирование на инциденты и отчеты. Кроме того, проверка безопасности информации должна проводиться регулярно, по крайней мере, один раз в год.

В рассматриваемом уведомлении содержится разработанное Банком Таиланда Руководство по безопасности информационных систем поставщиков услуг электронных платежей (Guidelines on Security of Information System Relating to Electronic Payment Service). Оно включает четыре раздела: 1) о контроле доступа и аутентификации (порядок назначения персонала или подразделения информационной системы, а также разделение полномочий при работе с информационной системой поставщиков услуг; осуществление контроля доступа к информационной системе; стандарты аутентификации и неотказуемости); 2) о конфиденциальности информации и целостности информационной системы (требования к конфиденциальности информации; регулирование и контроль версий информационной системы или оборудования обработки информации; управление сетью, связанное с работой услуги); 3) о доступности системы (порядок оценки рисков и управление операционной системой; обнаружение системы; реагирование на инцидент, запись и отчет в случае повреждения информационной системы; резервное копирование информации; план обеспечения непрерывности бизнеса или аварийный план информационной системы; обслуживание оборудования информационной системы); 4) о проверке безопасности информационной системы.

Общие требования к безопасности информационных систем Банк Таиланда установил в уведомлении о политике и мерах безопасности информационных систем (Bank of Thailand Notification No. SorNorChor. 11/2561 Re: Policies and Measures on Security of Information Technology Systems, URL: pttps://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/EngPDF/25610021.pdf&sa=U&ved=2a Этот документ определяет основные руководящие принципы безопасности: 1) контроль доступа и аутентификации; 2) конфиденциальность информации и целостность системы; 3) доступность услуг; 4) аудит безопасности информационных систем. Он должен быть

использован в качестве руководства при разработке комплекса мер безопасности информационных систем, относящихся к особо важным платежным системам, назначенным платежным системам и назначенным платежным услугам. Меры безопасности должны эффективно ликвидировать и предотвращать риски в соответствии с руководящими принципами международных стандартов. Кроме того, поставщики услуг особо важных платежных систем и бизнес-провайдеры платежных систем и услуг должны применять и разрабатывать меры безопасности информационных систем в зависимости от типов и сложности их собственных услуг.

Содержание четырех принципов раскрывается в утвержденном рассматриваемым уведомлением Руководстве по безопасности информационных систем, связанных с платежными системами (Guidelines on Security of IT Systems relating to the Payment Systems). Принцип контроля доступа и аутентификации определяет а) порядок назначения персонала или подразделений, ответственных за информационные технологии, и разделения обязанностей, соответствующих управлению информационными системами; б) контроль доступа к информационным системам; в) порядок проверки личности и предотвращение отказа от ответственности.

Принцип конфиденциальности информации и целостность системы определяет требования к 1) разработке систем, управлению контролем изменений, улучшению информационных систем или оборудования для обработки данных; 2) управлению сетевыми системами, относящимся к обслуживанию.

Доступность системы обеспечивается путем установления правил по а) оценке рисков и управлению системой обслуживания; б) мониторингу и обнаружению аномалий или уязвимостей информационных систем; в) разрешению, реагированию на инциденты, записи и отчетности в случае повреждения информационной системы; г) резервному копированию информации; д) разработке плана обеспечения непрерывности бизнеса или аварийного плана информационных систем; е) технического обслуживания оборудования информационных систем. Банк Таиланда требует проведения регулярного аудита безопасности информационных систем и осуществления обзора или улучшения мер безопасности информационных систем.

Выводы. В результате проведенного исследования мы пришли к следующим выводам. Полномочия финансового регулятора Таиланда распределены между тремя органами. Банк Таиланда контролирует коммерческие банки, финансовые компании, кредитные учреждения, компании по управлению активами, услуги электронных платежей и компании, выпускающие кредитные карты. Комиссия по ценным бумагам и биржевым операциям осуществляет надзор за операциями с ценными бумагами, в то время как Комиссия по страхованию - надзор за деятельностью страховых компаний. Обеспечение информационной безопасности возложено на Банк Таиланда, уполномоченного на создание системы управления рисками финансовых учреждений в целях обеспечения их стабильности. С этой целью он принимает нормативные акты, устанавливающие стандарты безопасности трех видов информационных систем: общего характера, обслуживающих электронные платежи и обслуживающих электронные платежные карты. Заслуживает внимания требование к операторам информационных систем при заключении соглашения об обслуживании определить права внутренних и внешних аудиторов, а также должностное лицо Банка Таиланда для проверки операций и контроля поставщика услуг. Финансовый регулятор определяет статус поставщиков услуг особо важных платежных систем, вменяя им в обязанность разрабатывать меры безопасности информационных систем в зависимости от типов и сложности их собственных услуг.

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. 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.
2. Горян Э.В. Нормативно-правовой механизм обеспечения безопасности киберпространства Таиланда // Вопросы безопасности. 2021. № 3. С. 1 – 20.
3. Аминов И.И. Предупреждение киберпреступлений в финансовой сфере / И.И. Аминов // Аллея науки. 2018. Т. 5. № 6 (22). С. 754-758.
4. Масленников В.В. Новые финансовые технологии меняют наш мир / В.В. Масленников, М.А. Федотова, А.Н. Сорокин // Вестник Финансового университета. 2017. Т. 21. № 2 (98). С. 6-11.
5. Молодцов Н.С. Компьютерные вирусы. Вирусные атаки 2017 года / Н.С. Молодцов, О.С. Клименко // Наука через призму времени. 2018. № 4 (13). С. 35-38.
6. Трифонова А.К. Кибератаки на банковский сектор: новые риски и пути преодоления / А.К. Трифонова, Р.Д. Бескровный // Экономика. Бизнес. Банки. 2017. № S2. С. 83-89.
7. Горян Э.В. Роль финансового регулятора в обеспечении кибербезопасности: опыт Сингапура // Финансовое право и управление. — 2018. - № 2. - С. 25-38.
8. Горян Э.В. Роль финансового регулятора в обеспечении кибербезопасности в России и Сингапуре: сравнительно-правовой аспект // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11. № 2. С.83–101.
9. Горян Э.В. Роль финансового регулятора в обеспечении информационной безопасности России и Китая: сравнительно-правовой аспект // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2020. – Т. 12. - № 2. – С. 88–102.

Результаты процедуры 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 «Роль финансового регулятора Таиланда в обеспечении информационной безопасности финансово-банковского сектора».
Предмет исследования. Предложенная на рецензирование статья посвящена вопросам о роли «…финансового регулятора Таиланда в обеспечении информационной безопасности финансово-банковского сектора». Автором выбран особый предмет исследования: предложенные вопросы исследуются с точки зрения права Таиланда, при этом автором отмечено, что «Координирующую роль в финансовом и банковском секторе играет финансовый регулятор, устанавливающий правила осуществления деятельности финансовыми институтами, в том числе в сфере обеспечения безопасности их

функционирования». Изучается законодательство Таиланда, которое представлено «нормативно-правовыми актами и источниками «мягкого права» Таиланда, устанавливающими требования к информационным системам субъектов финансово-банковского сектора», имеющее отношение к цели исследования. Также изучается и обобщается определенный объем научной литературы по заявленной проблематике, анализ и дискуссия с авторами-оппонентами отсутствует. При этом автор отмечает, что «Выбранная нами для исследования тема мало представлена в российской научной литературе», «…Таиланд проводит активное наращивание нормативно-правовой базы для регулирования процессов кибербезопасности».

Методология исследования. Цель исследования определена названием и содержанием работы: «…охарактеризовать роль финансового регулятора Таиланда – Банка Таиланда (Bank of Thailand), в обеспечении информационной безопасности финансово-банковского сектора. Задачи исследования заключаются в определении правового статуса финансового регулятора, его функций и характере сотрудничества с частным сектором в указанной сфере». Они могут быть обозначены в качестве рассмотрения и разрешения отдельных проблемных аспектов, связанных с вышеназванными вопросами и использованием определенного опыта. Исходя из поставленных цели и задач, автором выбрана определенная методологическая основа исследования. Автором используется совокупность общенаучных, специально-юридических методов познания «системно-структурный, формально-логический и формально-юридический методы». В частности, методы анализа и синтеза позволили обобщить некоторые подходы к предложенной тематике и отчасти повлияли на выводы автора. Наибольшую роль сыграли специально-юридические методы. В частности, автором применялся формально-юридический метод, который позволил провести анализ и осуществить толкование норм действующего законодательства. При этом в контексте цели исследования формально-юридический метод мог бы быть применен в совокупности со сравнительно-правовым методом, тем более автор об этом говорит: «Следует отметить, что отечественные научные исследования о роли российского финансового регулятора в обеспечении информационной безопасности банковской и финансовой систем публикуются регулярно, но компаративистические исследования в указанной сфере практически отсутствуют». В частности, делаются такие выводы: «Полномочия финансового регулятора Таиланда распределены между тремя органами. Банк Таиланда (Bank of Thailand, BOT) …. Комиссия по ценным бумагам и биржевым операциям (The Securities and Exchange Commission, SEC) …. Комиссия по страхованию (Office of Insurance Commission, OIC) …» и др. Таким образом, выбранная автором методология в полной мере адекватна цели статьи, позволяет изучить многие аспекты темы.

Актуальность заявленной проблематики не вызывает сомнений. Данная тема является одной из важных в мире и России, с правовой точки зрения предлагаемая автором работа может считаться актуальной, а именно он отмечает, что «…изучение опыта Таиланда по обеспечению кибербезопасности вообще [1; 2] и деятельности его финансового регулятора в рассматриваемой сфере в частности необходимо для совершенствования российского механизма кибербезопасности». И на самом деле здесь должен следовать анализ работ оппонентов и НПА, и он следует и автор показывает умение владеть материалом. Тем самым, научные изыскания в предложенной области стоит только приветствовать.

Научная новизна. Научная новизна предложенной статьи вызывает сомнения. Она не выражается в конкретных научных выводах автора. Среди них, например, такой: «Финансовый регулятор определяет статус поставщиков услуг особо важных платежных систем, вменяя им в обязанность разрабатывать меры безопасности информационных систем в зависимости от типов и сложности их собственных услуг». Как видно,

указанный и иные «теоретические» выводы не могут быть использованы в дальнейших научных исследованиях. Таким образом, материалы статьи в представленном виде могут иметь интерес для научного сообщества в качестве ознакомления с зарубежным НПА.

Стиль, структура, содержание. Тематика статьи соответствует специализации журнала «Национальная безопасность», так как посвящена вопросам о роли «…финансового регулятора Таиланда в обеспечении информационной безопасности финансово-банковского сектора». В статье присутствует аналитика по научным работам оппонентов, поэтому автор отмечает, что уже ставился вопрос, близкий к данной теме и автор использует их материалы, дискутирует с оппонентами. Содержание статьи соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели своего исследования. Качество представления исследования и его результатов следует признать доработанным. Из текста статьи прямо следуют предмет, задачи, методология, результаты юридического исследования, но не научная новизна. Оформление работы соответствует требованиям, предъявляемым к подобного рода работам. Существенные нарушения данных требований не обнаружены.

Библиография. Следует высоко оценить качество представленной и использованной литературы. Присутствие современной научной литературы и НПА (правда, ссылки на них не работают) показывает обоснованность выводов автора. Труды приведенных авторов соответствуют теме исследования, обладают признаком достаточности, способствуют раскрытию многих аспектов темы.

Апелляция к оппонентам. Автор провел серьезный анализ текущего состояния исследуемой проблемы. Автор описывает разные точки зрения оппонентов на проблему, аргументирует более правильную по его мнению позицию, опираясь на работы оппонентов, предлагает варианты решения отдельных проблем.

Выводы, интерес читательской аудитории. Выводы являются логичными, конкретными. Статья в данном виде может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к заявленным в статье вопросам. На основании изложенного, суммируя все положительные и отрицательные стороны статьи рекомендую «опубликовать» с учетом замечаний по научной новизне и выводов для РФ.