

INTERNATIONAL LAW JOURNAL

2021, Том 4, №6

Подписано к публикации: 05.11.2021

Главный редактор журнала
Серебренникова Анна Валерьевна
доктор юридических наук, профессор

Члены редакционной коллегии:

- Абшилава Георгий Валерьянович* (РФ, г. Ульяновск) – доктор юридических наук, профессор
Авакян Рубен Осипович (Армения, г. Ереван) – доктор юридических наук, профессор
Айбатов Магомеднаби Магомедмирзоевич (РФ, Р. Дагестан) – доктор юридических наук, профессор
Белоцеркович Денис Валерьевич (РФ, г. Хабаровск) – кандидат юридических наук, доцент
Бирюков Павел Николаевич (РФ, г. Воронеж) – доктор юридических наук, профессор
Василевич Григорий Алексеевич (Беларусь, г. Минск) – доктор юридических наук, профессор
Васильев Сергей Владимирович (РФ, г. Псков) – доктор юридических наук, профессор
Васильев Федор Петрович (РФ, г. Москва) – доктор юридических наук, профессор
Глебов Игорь Николаевич (РФ, г. Москва) – доктор юридических наук, профессор
Громов Владимир Геннадьевич (РФ, г. Саратов) – доктор юридических наук, профессор
Джаллилов Эльвис Алимович (РФ, г. Тольятти) – кандидат юридических наук, доцент
Жамулдинов Виктор Николаевич (Казахстан, г. Павлодар) – кандидат юридических наук, доцент
Захарова Светлана Александровна (РФ, Екатеринбург) – кандидат юридических наук, доцент
Ибрагимов Жамаладен Ибрагимович (Казахстан, г. Астана) – доктор юридических наук, профессор
Кириллова Ирина Александровна (РФ, г. Курск) – кандидат юридических наук, доцент
Коваленко Вадим Николаевич (РФ, г. Волгоград) – доктор юридических наук, профессор
Кожневников Олег Александрович (РФ, г. Екатеринбург) – доктор юридических наук, доцент
Коршунова Ольга Николаевна (РФ, г. Санкт-Петербург) – доктор юридических наук, профессор
Лазарева Лариса Владимировна (РФ, г. Владимир) – доктор юридических наук, профессор
Машовец Асия Океановна (РФ, г. Ульяновск) – доктор юридических наук, доцент
Мельников Николай Николаевич (РФ, г. Орёл) – доктор юридических наук, доцент
Миняева Татьяна Федоровна (РФ, г. Москва) – доктор юридических наук, профессор
Миронов Анатолий Николаевич (РФ, г. Москва) – доктор юридических наук, профессор
Михайлова Екатерина Владимировна (РФ, г. Москва) – доктор юридических наук, доцент, ведущий научный сотрудник
Мишина Наталья Вячеславовна (РФ, г. Москва) – доктор политических наук, доцент
Мустафаева Айтен Инглаб (Азербайджан, г. Баку) – доктор юридических наук, профессор
Небрятенко Геннадий Геннадьевич (РФ, г. Ростов-на-Дону) – доктор юридических наук, профессор
Николайченко Виктор Викторович (РФ, г. Саратов) – доктор юридических наук, профессор,
Остапович Игорь Юрьевич (РФ, г. Барнаул) – доктор юридических наук, доцент
Пешкова Христина Вячеславовна (РФ, г. Воронеж) – доктор юридических наук, профессор
Русинова Вера Николаевна (РФ, г. Москва) – доктор юридических наук, профессор
Сумачев Алексей Витальевич (РФ, г. Ханты-Мансийск) – доктор юридических наук, профессор
Халифаева Анжела Курбановна (РФ, Р. Дагестан) – доктор юридических наук, профессор
Числов Александр Иванович (РФ, г. Тюмень) – доктор юридических наук, профессор
Файзиев Шохруд Фармонович (Узбекистан, г. Ташкент) – кандидат юридических наук, доцент
Флоря Евгений Константинович (Молдова, г. Кишинев) – кандидат юридических наук, доцент
Шатковская Татьяна Владимировна (РФ, г. Ростов-на-Дону) – доктор юридических наук, профессор
Шошин Сергей Владимирович (РФ, г. Саратов) – кандидат юридических наук, доцент

«International Law Journal» включен в список ВАК с 25.12.2020г., РИНЦ (Elibrary.ru)

Свидетельство о регистрации СМИ: Эл № ФС77-78049 от 4 марта 2020г. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

ISSN 2658-5693 (online)

E-mail: law@dgpu-journals.ru

Сайт: <http://ilj-journal.ru>

© International Law Journal, 2021

Содержание

Кулапова Т.Ю. ПРОБЛЕМЫ АНТИКОРРУПЦИОННОЙ ПОЛИТИКИ ОРГАНИЗАЦИЙ	9-12
Виннер Э.Р. УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НЕДОБРОСОВЕСТНУЮ ЭМИССИЮ ЦЕННЫХ БУМАГ	13-17
Тронина Е.Г. КОНСТИТУЦИОННЫЕ ОСНОВЫ ВОСПИТАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ	18-20
Зубков И.Б. ПРАВОВЫЕ ПОСЛЕДСТВИЯ УТРАТЫ ИЛИ ИСКАЖЕНИЯ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ	21-25
Рахмон Каландаршохи ИСТОРИЧЕСКИЕ И ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ СТАНОВЛЕНИЯ И РАЗВИТИЯ ПРОКУРОРСКОГО НАДЗОРА ЗА ИСПОЛНЕНИЕМ ЗАКОНОВ ОРГАНАМИ ГОСУДАРСТВЕННОЙ ВЛАСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКЕ ТАДЖИКИСТАН	26-30
Гатауллин З.Ш. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПОДОЗРЕВАЕМОГО (ОБВИНЯЕМОГО) В СОВЕРШЕНИИ ПРЕСТУПЛЕНИЯ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ ЗАКЛЮЧИВШЕГО ДОСУДЕБНОЕ СОГЛАШЕНИЕ О СОТРУДНИЧЕСТВЕ	31-34
Коноплева Ю.А. К ВОПРОСУ О НАЗНАЧЕНИИ ПЕНСИИ НЕКОТОРЫМ КАТЕГОРИЯМ ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ	35-38
Кужеков А.Ю., Абражеева Д.В. К ВОПРОСУ О ВЗАИМОДЕЙСТВИИ ПРАВА И НРАВОВ В ПЕНИТЕНЦИАРНОЙ СИСТЕМЕ	39-41
Николаев Д.А. ОСНОВАНИЯ ВОЗНИКНОВЕНИЯ ПРЕДПРИНИМАТЕЛЬСКИХ ПРАВООТНОШЕНИЙ В СФЕРЕ ДОБЫЧИ ОБЩЕРАСПРОСТРАНЕННЫХ ПОЛЕЗНЫХ ИСКОПАЕМЫХ	42-46
Парфенов М.Р. К ВОПРОСУ ВЛИЯНИЯ МОДЕРНИЗАЦИИ И ЦИФРОВИЗАЦИИ ПРОЦЕССА РЕГИСТРАЦИИ НЕДВИЖИМОГО ИМУЩЕСТВА НА СИСТЕМУ ПРЕДУПРЕЖДЕНИЯ МОШЕННИЧЕСТВА В СФЕРЕ ОБОРОТА НЕДВИЖИМОСТИ	47-51
Шубников Ю.Б., Кузин Н.Н., Рашидова А.И. СИСТЕМНЫЕ АСПЕКТЫ ПРЕДПРИНИМАТЕЛЬСКОГО ПРАВА	52-58
Репин А.В. ПРЕКРАЩЕНИЕ ДОГОВОРА ПОДРЯДА В СЛУЧАЕ ВВЕДЕНИЯ ПРОЦЕДУРЫ КОНКУРСНОГО ПРОИЗВОДСТВА В ОТНОШЕНИИ ОДНОЙ ИЗ СТОРОН ДОГОВОРА	59-62

Сергеева К.А., Юртаев В.А. ПРАВОСУДИЕ И ПАНДЕМИЯ КОРОНАВИРУСА: ВЫНУЖДЕННАЯ ЦИФРОВИЗАЦИЯ	63-68
Шакурова Н.К. ВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ ПОЛОЖЕНИЙ СТАТЬИ 1079 ГК РФ К СИТУАЦИИ ОСТАНОВКИ И СТОЯНКИ ТРАНСПОРТНОГО СРЕДСТВА В МОМЕНТ ДОРОЖНО- ТРАНСПОРТНОГО ПРОИСШЕСТВИЯ	69-72
Ямковая И.Н. ПОНЯТИЕ НАРОДНОГО СУВЕРЕНИТЕТА В КОНТЕКСТЕ АНАЛИЗА ТЕОРИИ НАРОДОВЛАСТИЯ	73-77
Барышников М.Ю. САМОЗАЩИТА КАК ЭЛЕМЕНТ МЕХАНИЗМА РЕАЛИЗАЦИИ И ЗАЩИТЫ ТРУДОВЫХ ПРАВ В СИСТЕМЕ ЧАСТНЫХ ПРАВООТНОШЕНИЙ РОССИИ И ЗАРУБЕЖНЫХ ГОСУДАРСТВ	78-83
Васяев А.А. АВТОНОМИЯ ВОЛИ КАК СПОСОБ ВЫРАЖЕНИЯ КОЛЛИЗИОННО- ПРАВОВОЙ СВОБОДЫ УЧАСТНИКОВ ДОГОВОРНЫХ ОТНОШЕНИЙ В МЕЖДУНАРОДНОМ ЧАСТНОМ ПРАВЕ	84-89
Завгороднева Е.В. СОСТАВЛЯЮЩИЕ ПРОЦЕССА ДОКАЗЫВАНИЯ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ	90-96
Абезин Д.А., Мохов А.Ю., Абезин Д.Д. ПРАВОВАЯ РЕГЛАМЕНТАЦИЯ ГРАДОСТРОИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ДОРЕВОЛЮЦИОННОЙ РОССИИ: ОСНОВНЫЕ ЭТАПЫ	97-102
Муцалов Ш.Ш., Шахбиева Х.А. ИССЛЕДОВАНИЕ СУЩНОСТИ, ПОНЯТИЯ И КЛАССИФИКАЦИИ НОРМ ЮРИДИЧЕСКОЙ ПОЛИТИКИ	103-108
Николаев Д.А. ОСОБЕННОСТИ ПРЕДПРИНИМАТЕЛЬСКИХ ПРАВООТНОШЕНИЙ В СФЕРЕ ДОБЫЧИ ОБЩЕРАСПРОСТРАНЕННЫХ ПОЛЕЗНЫХ ИСКОПАЕМЫХ	109-112
Блинова О.А., Девятковская И.В. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ВАНДАЛЬНОГО ПОВЕДЕНИЯ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА РОССИИ, БЕЛАРУСИ И ГЕРМАНИИ	113-120
Гитинова М.М., Шамхалов К.Н. К ВОПРОСУ О СПЕЦИФИЧНЫХ ПРИНЦИПАХ УГОЛОВНОГО ПРАВА	121-124
Магомедова Е.А., Денисов И.М., Лещинский М.И. ЗАКРЕПЛЕНИЕ ПРАВИЛ ЗАКОНОДАТЕЛЬНОЙ ТЕХНИКИ В ЗАКОНОДАТЕЛЬСТВЕ СУБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРОБЛЕМНЫЕ АСПЕКТЫ	125-130

Васенёв М.И., Любенко Ю.В. ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПО ДЕЛАМ О ВЗЫСКАНИИ УБЫТКОВ В ДОГОВОРНОМ ПРАВЕ	131-135
Горян Э.В. ВЗАИМОСВЯЗЬ ПРАВОВОГО РЕЖИМА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И ОБЕСПЕЧЕНИЯ ПРАВ ИНВЕСТОРОВ (НА ПРИМЕРЕ РОССИИ, КИТАЯ И ТАИЛАНДА)	136-141
Жуковская Н.Ю., Чепрасова Ю.В. ПРОБЛЕМЫ ЮРИДИЧЕСКОЙ ОЦЕНКИ МОЛОДЕЖНОГО РАДИКАЛИЗМА И РОЛЬ ПРАВОВОГО ВОСПИТАНИЯ В ЕГО ПРОФИЛАКТИКЕ	142-146
Квач С.С., Федулов И.Н., Романова Т.И. О ПОНЯТИЯХ «ИСТОЧНИК ПРАВА» И «ИСТОЧНИК МУНИЦИПАЛЬНОГО ПРАВА»	147-150
Халифаева А.К., Айбатов М.М., Чаканаев М.Р., Алиев А.М. К ВОПРОСУ ОБ ИСТОРИИ СУДЕБНОГО ПРИСТАВА И ОРГАНОВ ПРЕДВАРИТЕЛЬНОГО СЛЕДСТВИЯ	151-155
Бессарабова С.Ю. СРОЧНЫЙ ХАРАКТЕР СЕМЕЙНЫХ ПРАВООТНОШЕНИЙ	156-161

Contents

Kulapova T.Yu. PROBLEMS OF ANTI-CORRUPTION POLICIES OF ORGANIZATIONS	9-12
Vinner E.R. CRIMINAL RESPONSIBILITY FOR UNFAIR SECURITIES ISSUE	13-17
Tronina E.G. CONSTITUTIONAL FOUNDATIONS OF EDUCATION IN THE RUSSIAN FEDERATION	18-20
Zubkov I.B. LEGAL CONSEQUENCES OF THE LOSS OR DISTORTION OF INFORMATION CONTAINED IN STATE INFORMATION SYSTEMS	21-25
Rakhmon Kalandarshokhi HISTORICAL AND THEORETICAL ASPECTS OF THE FORMATION AND DEVELOPMENT OF PROSECUTOR'S SUPERVISION OVER THE EXECUTION OF LAWS BY STATE AUTHORITIES IN THE RUSSIAN FEDERATION AND THE REPUBLIC OF TAJIKISTAN	26-30
Gataullin Z.Sh. ENSURING THE SECURITY OF THE SUSPECT (ACCUSED) IN THE COMMISSION OF A TERRORIST CRIME THAT CONCLUDED A PRE-TRIAL COOPERATION AGREEMENT	31-34
Konopleva Yu.A. ON THE ISSUE OF ASSIGNING PENSIONS TO CERTAIN CATEGORIES OF TEACHING STAFF	35-38
Kuzhekov A.Yu., Abrazheeva D.V. ON THE QUESTION OF THE INTERACTION OF LAW AND MORALS IN THE PENITENTIARY SYSTEM	39-41
Nikolaev D.A. REASONS FOR THE EMERGENCE OF BUSINESS LEGAL RELATIONS IN THE FIELD OF EXTRACTION OF COMMON MINERALS	42-46
Parfenov M.R. ON THE ISSUE OF THE IMPACT OF MODERNIZATION AND DIGITALIZATION OF THE REAL ESTATE REGISTRATION PROCESS ON THE FRAUD PREVENTION SYSTEM IN THE SPHERE OF REAL ESTATE TURNOVER	47-51
Shubnikov Yu.B., Kuzin N.N., Rashidova A.I. SYSTEMIC ASPECTS OF BUSINESS LAW	52-58
Repin A.V. TERMINATION OF THE CONTRACT IN THE EVENT OF THE INTRODUCTION OF A BANKRUPTCY PROCEDURE IN RESPECT OF ONE OF THE PARTIES TO THE CONTRACT	59-62
Sergeeva K.A., Yurtaev V.A. JUSTICE AND THE CORONAVIRUS PANDEMIC: FORCED DIGITALISATION	63-68

Shakurova N.K. THE POSSIBILITY OF APPLYING THE PROVISIONS OF ARTICLE 1079 OF THE CIVIL CODE OF THE RUSSIAN FEDERATION TO THE SITUATION OF STOPPING AND PARKING A VEHICLE AT THE TIME OF A TRAFFIC ACCIDENT	69-72
Yamkovaya I.N. THE CONCEPT OF NATIONAL SOVEREIGNTY IN THE CONTEXT OF THE ANALYSIS OF THE THEORY OF DEMOCRACY	73-77
Baryshnikov M.Yu. SELF-DEFENSE AS AN ELEMENT OF THE MECHANISM FOR THE IMPLEMENTATION AND PROTECTION OF LABOR RIGHTS IN THE SYSTEM OF PRIVATE LEGAL RELATIONS OF RUSSIA AND FOREIGN STATES	78-83
Vasyaev A.A. AUTONOMY OF WILL AS A WAY OF EXPRESSING THE CONFLICT OF LAW FREEDOM OF THE PARTIES TO CONTRACTUAL RELATIONS IN PRIVATE INTERNATIONAL LAW	84-89
Zavgorodneva E.V. COMPONENTS OF THE PROOF PROCESS IN CRIMINAL PROCEEDINGS	90-96
Abezin D.A., Mokhov A.Yu., Abezin D.D. LEGAL REGULATION OF URBAN PLANNING ACTIVITIES IN PRE-REVOLUTIONARY RUSSIA: MAIN STAGES	97-102
Mutsalov Sh.Sh., Shakhbieva H.A. INVESTIGATION OF THE ESSENCE, CONCEPT AND CLASSIFICATION OF LEGAL POLICY NORMS	103-108
Nikolaev D.A. FEATURES OF BUSINESS LEGAL RELATIONS IN THE FIELD OF EXTRACTION OF COMMON MINERALS	109-112
Blinova O.A., Devyatovskaya I.V. LEGAL REGULATION OF VANDAL BEHAVIOR: COMPARATIVE ANALYSIS OF THE CRIMINAL LEGISLATION OF RUSSIA, BELARUS AND GERMANY	113-120
Gitinova M.M., Shamkhalov K.N. ON THE QUESTION ABOUT SPECIFIC PRINCIPLES OF CRIMINAL LAW	121-124
Magomedova E.A., Denisov I.M., Leshchinsky M.I. FIXING THE RULES OF LEGISLATIVE TECHNIQUE IN THE LEGISLATION OF THE SUBJECTS OF THE RUSSIAN FEDERATION: PROBLEMATIC ASPECTS	125-130
Vasenev M.I., Lyubenko Yu.V. FEATURES OF EVIDENCE IN CASES OF RECOVERY OF DAMAGES IN CONTRACT LAW	131-135

Goryan E.V. CORRELEATION OF THE CRITICAL INFORMATION INFRASTRUCTURE OF LEGAL REGIME AND THE INVESTORS RIGHTS' ENFORCEMENT (THE CASE OF RUSSIA, CHINA, AND THAILAND)	136-141
Zhukovskaya N.Yu., Cheprasova Yu.V. PROBLEMS OF LEGAL ASSESSMENT OF YOUTH RADICALISM AND THE ROLE OF LEGAL EDUCATION IN ITS PREVENTION	142-146
Kvach S.S., Fedulov I.N., Romanova T.I. ON THE CONCEPTS OF "SOURCE OF LAW" AND "SOURCE OF MUNICIPAL LAW"	147-150
Halifaeva A.K., Aibatov M.M., Chakanaev M.R., Aliev A.M. TO THE QUESTION OF THE HISTORY OF THE BAILIFF AND THE PRELIMINARY INVESTIGATION BODIES	151-155
Bessarabova S.Yu. THE URGENT NATURE OF FAMILY LEGAL RELATIONS	156-161

**ВЗАИМОСВЯЗЬ ПРАВОВОГО РЕЖИМА КРИТИЧЕСКОЙ
ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И ОБЕСПЕЧЕНИЯ ПРАВ
ИНВЕСТИТОРОВ (НА ПРИМЕРЕ РОССИИ, КИТАЯ И ТАИЛАНДА)**

**Горян Э.В., кандидат юридических наук, доцент,
Владивостокский государственный университет экономики и сервиса**

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»

Аннотация: предметом исследования выступают нормативно-правовые акты России, Китая и Таиланда в сфере обеспечения информационной безопасности и регулирования инвестиционных отношений, определяющие правовой режим критической информационной инфраструктуры. Цель исследования – определение особенностей правовых режимов критической информационной инфраструктуры в России, Китае и Таиланде в аспекте обеспечения прав инвесторов. Задачи: охарактеризовать правовые режимы критической информационной инфраструктуры в каждом из государств; выделить особые черты, влияющие на инвестиционную привлекательность финансово-банковского сектора этих государств. Сделан вывод о том, что правовая определенность и отсутствие пробелов в законодательстве являются основными факторами, влияющими на инвестиционный режим в государстве. Из трех рассматриваемых юрисдикций две (Россия и Таиланд) характеризуются высокими параметрами указанных факторов, что прямо влияет на инвестиционный климат и привлекает инвесторов. В Китае уровень решающих параметров ниже, что можно объяснить особой правовой системой и сложной внешнеполитической ситуацией: многолетними торговыми спорами с США, которые реализуют политику экономической экспансии на информационно-технологический рынок Китая, используя в качестве рычагов давления тарифные и нетарифные меры. Следовательно правовой режим критической информационной инфраструктуры может быть использован в качестве действенной меры по защите внутреннего рынка государства и стимулирования внутреннего и зарубежного инвестирования.

Ключевые слова: кибербезопасность, критическая информационная инфраструктура, права инвесторов, финансово-банковский сектор, правовой режим, правовые гарантии

**CORRELEATION OF THE CRITICAL INFORMATION INFRASTRUCTURE
OF LEGAL REGIME AND THE INVESTORS RIGHTS' ENFORCEMENT
(THE CASE OF RUSSIA, CHINA, AND THAILAND)**

**Goryan E.V., Candidate of Juridical Sciences (Ph.D.), Associate Professor,
Vladivostok State University of Economics and Service**

Abstract: the subject of the research is the legislation of Russia, China and Thailand in the sphere of information security and investment regulation, which determines the legal regime of critical information infrastructure. The purpose of the study is to determine the features of the critical information infrastructure legal regimes in Russia, China and Thailand in terms of investors rights' enforcement, i.e. to characterize the national critical information infrastructure legal regimes; to highlight the special features affecting the investment attractiveness of the financial and banking sectors. It is concluded that legal positiveness and the absence of legal lacunas are the core factors affecting the national investment regime. Two of the three jurisdictions (Russia and Thailand) perform the high parameters of the abovementioned factors, which directly affect the investment climate and attracts investors. China performs the comparatively lower level of decisive parameters, that is explained by a specific legal system and a complex foreign policy situation: the years of trade disputes with the United States, which promote a policy of economic expansion into the Chinese information technology market, using tariff and non-tariff measures as a leverage. Therefore, the critical information infrastructure legal regime can be used as an effective measure to protect the national markets and to stimulate domestic and foreign investments.

Keywords: cybersecurity, critical information infrastructure, investors rights, financial and banking sector, legal regime, legal guarantees

Актуальность темы исследования

Информация стала новым нематериальным активом в современной экономике, что привело к ее цифровизации и зависимости материальных активов от степени сохранности и защищенности от посягательств. Более того, эти качества информации, представленной в виде данных, влияют на инвестиционную привлекательность как тех или иных сегментов экономики, так и государств. С учетом этих факторов государства разрабатывают и развивают модели обеспечения безопасности в информационной сфере, служащие ориентирами для других государств в развитии своих правовых систем. Особый интерес представляют государства Азии, показывающие двойные показатели роста цифровой экономики (с 50 до 100 млрд долларов США) [1]. Финансовые услуги наряду с электронной торговлей (e-Commerce) и транспортными услугами/доставкой еды являются ведущими секторами цифровой экономики, что делает их привлекательными объектами для инвестирования. Но инвестиции требуют особых гарантий со стороны государства, как нормативно-правовых и организационно-правовых, так и институциональных. Например, 2021 год запомнится беспрецедентными мерами китайских властей по привлечению к ответственности крупнейшего агрегатора такси Didi и других компаний сферы BigTech за ряд нарушений, в том числе в сфере персональных данных и антимонопольного законодательства, что повлекло за собой делистинг акций на биржах США [2], с последующими спадом инвестиционной активности. Финансово-банковский сектор как яркий представитель сферы BigTech является ключевым объектом критической информационной инфраструктуры, поэтому все события, происходящие с ним, прямо или косвенно влияют на инвестиционные отношения и определяют инвестиционный климат в государстве. Поэтому государство берет на себя дополнительные положительные обязательства по обеспечению информационной безопасности учреждений финансово-банковского сектора с целью обеспечения прав инвесторов.

Постановка проблемы исследования

Инвестиционный климат государства определяется множеством факторов – политических, правовых, институциональных, экономических и других. BigTech и FinTech являются одними из наиболее популярных сфер инвестирования, а учитывая их цифровую природу, завязанную на информационно-компьютерных технологиях, к «стандартным» инвестиционным рискам добавляются риски технологические, избежать которых можно путем применения в том числе и организационно-правовых мер, направленных на защиту информационных систем. Международным сообществом было безоговорочно признана необходимость установления специального правового режима для критической информационной инфраструктуры (далее по тексту - КИИ) для учреждений финансово-банковского сектора, однако подходы к правовому регулированию государств могут отличаться по всевозможным причинам, прежде всего как по внешне- и внутривластным, так и экономическим. Поэтому строгость правового режима КИИ непосредственно влияет на инвестиционный климат в государстве и, как следствие, на степень обеспеченности прав инвесторов.

Цель и задачи

Целью исследования является определение особенностей правовых режимов КИИ в России, Китае и Таиланде в аспекте обеспечения прав инвесторов. Достижение поставленной цели возможно при решении следующих задач: исследовать национальные правовые режимы КИИ; выделить особые черты, влияющие на инвестиционную привлекательность финансово-банковского сектора этих государств.

Методология и предмет исследования

Поставленная цель определяет выбор методов научного познания, как общенаучных, так и специальных юридических. В первом случае это системно-структурный и формально-логический методы, во втором – сравнительно-правовой и формально-юридический. Выбор рассматриваемых правовых систем определяется их ролью и амбициями в международных отношениях как глобального, так и регионального характера. В частности, Россия и Китай реализуют модель так называемого «цифрового национализма», которая характеризуется повышенной ответственностью государства за обеспечение безопасности информации и информационных систем (в том числе КИИ), находящей свое воплощение во введении особых правовых режимов оборота и защиты данных, включая персональные. Оба государства усиливают свое политическое и экономическое присутствие в юго-восточной Азии, участвуя в большинстве проектов Ассоциации государств Юго-Восточной Азии (АСЕАН) и в рамках двустороннего сотрудничества с лидерами региона. Несмотря на то, что ключевая роль в регионе принадлежит Сингапуру, последние годы Таиланд, входящий в двадцатку государств мира, занимающих лидирующие позиции в обеспечении кибербезопасности [3], оспаривает его лидерство, предпринимая ряд успешных международных и внутривластных инициатив [4], благодаря которым он ежегодно поднимается в Мировом рейтинге цифровой конкурентоспособности (World Digital Competitiveness Rankings [5]). В качестве предмета исследования использовано законодательство России, Китая и Таиланда, устанавливающее правовой режим КИИ.

Результаты исследования

В теории права правовой режим определяется как «специальный закрепленный в нормативно-правовых актах различного уровня порядок регулирования общественных отношений, основанный на установленных и обеспеченных государством правовых средствах, направленный на формирование благоприятных условий для удовлетворения интересов субъектов права, выражающийся в специфике способов и гарантий его реализации, ответственности за нарушение его требований и основывается на действии общих принципов, приводящих все его элементы в единую упорядоченную систему» [6, с. 33]. К таким гарантиям относят не только нормативно-правовые акты, закрепляющие правила поведения обязанных субъектов (нормативные гарантии), но и самих государственных органов и их должностных лиц, уполномоченных осуществлять правоприменительную деятельность, основанную на таких юридических нормах (институциональные гарантии) [7, с. 22]. Гарантии представляют собой условия осуществления прав субъектов, поэтому наличие необходимых гарантий прямо влияет на уровень обеспеченности таких прав. Соответственно существует прямая зависимость между наличием и совершенством правового режима и степенью обеспеченности прав субъекта. Как отмечалось нами в предыдущих исследованиях [8], к учреждениям финансово-банковского сектора применяется специальный правовой режим регулирования информационной безопасности, поскольку этот сектор считается частью КИИ во всех государствах мира. Действие этого правового режима происходит в результате функционирования правового механизма, поэтому утверждение о прямой взаимосвязи эффективной работы механизма обеспечения безопасности КИИ с уровнем обеспеченности прав инвесторов в финансово-банковском секторе бесспорно.

Правовой режим КИИ, регламентируемый федеральным законодательством России, является одним из совершенных в мире. Прежде всего, законодатель разработал специальный закон (Федеральный закон Российской Федерации от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», далее – ФЗ-187), устанавливающий нормативные и институциональные элементы правового механизма обеспечения безопасности КИИ. Нормативные элементы, выступающие в качестве основных гарантий, предусматривают закрытый перечень секторов КИИ, объекты которых могут подпадать под сферу применения правового режима КИИ (п. 8 ст. 2) и нарушение работы которых может поставить под угрозу безопасность и благополучие личности, общества и государства. Следует отметить, что перечень секторов, определенных Россией, перекликается с рекомендациями Агентства кибербезопасности ЕС (ENISA) для государств-участников Евросоюза и включает также финансово-банковский сектор. Специальные нормативные гарантии закреплены в подзаконных нормативных актах, принятых во исполнение ФЗ-187 Правительством РФ, Федеральной службой технического и экспортного контроля, Федеральной службой безопасности и проч. Особо следует отметить введение новеллы в Уголовный кодекс Российской Федерации – криминализацию деяний в отношении объектов КИИ (ст. 274.1). Правовой режим КИИ объектов финансово-банковского сектора дополняется специальными нормами, разрабатываемыми финансовым регулятором – Центральным банком России [9].

В качестве институциональных гарантий выступают органы государственной власти, определенные в ФЗ-187 и наделенные соответствующими полномочиями: как общей компетенции (Президент России, Правительство Российской Федерации и др.), так и специальной. Причем органы специальной компетенции можно разделить на две группы: первая группа формирует специальную государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ФСБ России, Национальный координационный центр по компьютерным инцидентам), а вторая группа представлена органами власти, специализирующимися на определенных аспектах информационной безопасности (ФСТЭК, Минкомсвязи, Центральный банк России).

В Китае правовой режим КИИ основывается на положениях Закона о кибербезопасности КНР 2016 года, а также ряде подзаконных нормативных актов и стандартов, принимаемых органами общей и специальной компетенции [10]. Китайский подход к определению КИИ характеризуется установлением открытого перечня секторов КИИ в законе, дополняемый положениями подзаконных нормативных актов. Как и Россия, Китай довольно широко определяет перечень секторов КИИ (в том числе и финансово-банковский), оставляя за собой право в случаях необходимости включать подзаконными нормативными актами дополнительные, если они имеют существенное значение для государства, общества, экономики и граждан (ст. 31) [11]. Особенностью правового режима КИИ Китая является длительный процесс разработки, обсуждения и утверждения подзаконных нормативных актов органами исполнительной власти, что создает некую неопределенность для потенциальных операторов КИИ (а следовательно и инвесторов). Например, четыре года потребовалось для утверждения Регламента защиты критической информационной инфраструктуры [12], который детально определяет перечень секторов и признаки, по которым можно идентифицировать новые сектора КИИ; обязательства операторов КИИ; нормативные требования по защите КИИ; уголовные

и административные санкции за нарушения режима КИИ операторами. Длительность законодательного процесса негативно влияет на инвестиционный климат в отношении потенциальных объектов для инвестиций.

В Законе о кибербезопасности КНР отсутствуют нормы, определяющие институциональные гарантии. Анализ нормативно-правовой базы обеспечения информационной безопасности позволяет выделить органы общей (Госсовет Китая, Министерство общественной безопасности и Министерство промышленности и информационных технологий) и специальной компетенции (Администрация киберпространства Китая, уполномоченная осуществлять общее руководство безопасностью ключевых секторов экономики – финансово-банковской системы, транспортной и энергетической). В финансово-банковском секторе наблюдается дублирование полномочий государственных структур, формирующих систему финансового регулирования (финансовый регулятор в Китае представлен не одним органом, как в России или Таиланде: Комитетом по финансовой стабильности и развитию при Государственном совете КНР, Народным банком Китая и Комиссией по регулированию банковского страхования), что негативно отображается на правовом режиме КИИ, характеризующегося на данный момент правовой неопределенностью [10].

В Таиланде правовой режим КИИ основывается на положениях Закона о кибербезопасности Таиланда 2019 года, Уголовного кодекса Таиланда, Закона об электронных операциях 2001 года, Закона о финансовых операциях 2008 года, Закона о телекоммуникационных операциях и Закона о платежных системах 2017 года.

Критическая информационная инфраструктура, определенная в Законе о кибербезопасности Таиланда 2019 года [13], включает секторы, важные для национальной, военной и экономической безопасности, а также общественного порядка: 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 здоровье и другие, которые определит Национальный комитет по кибербезопасности (National Cybersecurity Committee). Он также уполномочен назначать членов Комитета по регулированию кибербезопасности (Cybersecurity Regulating Committee), который разрабатывает минимальные стандарты кибербезопасности.

Институциональные гарантии представлены также следующими органами государственной власти, уполномоченными выполнять функцию регулирования кибербезопасности КИИ в соответствующем секторе: 1) Комитет по защите персональных данных в рамках реализации Закона о защите персональных данных 2019 года [14]; 2) Банк Таиланда в качестве финансового регулятора в отношении финансовых учреждений и поставщиков услуг электронных платежей; 3) Комиссия по ценным бумагам и биржам Таиланда; 4) Национальная комиссия по телерадиовещанию и телекоммуникациям. Указанные органы уполномочены принимать подзаконные нормативные акты, обязательные к применению операторами КИИ для обеспечения информационной безопасности и выступающие в качестве дополнительных нормативных гарантий прав инвесторов. В частности, в сфере финансово-банковской деятельности поставщики финансовых услуг должны соблюдать предписания Банка Таиланда относительно мер цифровой безопасности и управления рисками. В соответствии с Законом о платежных системах Таиланда 2017 года [15] поставщики услуг электронных платежей также должны соблюдать предписания Банка Таиланда, касающиеся управления непрерывностью бизнеса и оценки рисков, в частности, в отношении наличия плана действий в чрезвычайных обстоятельствах или системы резервных политик для обеспечения непрерывности обслуживания, а также политик безопасности и мер для используемых информационных систем.

Выводы

Правовая определенность и отсутствие пробелов в законодательстве являются основными факторами, влияющими на инвестиционный режим в государстве. Учитывая растущий интерес инвесторов к таким сегментам цифровой экономики, как финансы и банковское дело, а также электронная торговля, активность инвесторов напрямую зависит от степени инвестиционных рисков, которые представлены в большей степени информационно-технологическими. Из трех рассматриваемых юрисдикций две (Россия и Таиланд) характеризуются высокими параметрами указанных факторов, что прямо влияет на инвестиционный климат и привлекает инвесторов. Китай реализует политику «цифрового национализма», которая в совокупности с особой правовой системой замедляет, если не препятствует приходу иностранных (прежде всего из США) инвесторов на информационно-технологический рынок путем установления правового режима, отличающегося непрозрачностью и неоднозначностью толкования. Такой подход Китая оправдан стремлением защитить внутренний рынок от экономической экспансии США и обеспечить национальную безопасность государства. Следовательно правовой режим критической информационной инфраструктуры может быть использован в качестве действенной меры по защите внутреннего рынка государства и стимулирования внутреннего и зарубежного инвестирования.

Литература

1. e-Conomy SEA Spotlight 2020. At full velocity: Resilient and racing ahead [Electronic resource] // Google e-Conomy SEA 2020. [2021]. URL: <https://economysea.withgoogle.com/#explore> (retrieved: 14.11.2021)
2. Lockett H. Chinese tech stocks fall sharply on rising regulatory concerns [Electronic resource] // Financial Times. [2021]. URL: <https://www.ft.com/content/7bacf9ef-4ba0-4d5f-a471-144432847f57> (retrieved: 14.11.2021)
3. Toomgum S. Thailand among top 20 nations focusing on cybersecurity [Electronic resource] // The Nation. [2017]. URL: <http://www.nationmultimedia.com/detail/Economy/30325029> (retrieved: 14.11.2021)
4. Горян Э.В. Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2018. Т. 10. № 3. С. 103 – 117.
5. IMD World Digital Competitiveness Ranking 2020 [Electronic resource] // IMD World Competitiveness Center. [2021]. URL: <https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/> (retrieved: 14.11.2021).
6. Беляева Г.С. Правовой режим: к определению понятия // Исторические, философские, политические и юридические науки, культурология и искусствоведение: Вопросы теории и практики. 2012. Т. 17. № 3. Ч. 2. С. 33 – 35.
7. Сергеева Е.И. Юридические гарантии в системе гарантий прав личности в Российской Федерации // Закон. Право. Государство. 2019. № 2 (22). С. 22 – 26.
8. Горян Э.В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект // Административное и муниципальное право. 2018. № 9. С. 49 – 60.
9. 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.
10. 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.
11. Cybersecurity Law of the People's Republic of China [Electronic resource] // pkulaw.com. [2021]. URL: https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html (retrieved: 14.11.2021)
12. The Regulations on the Security and Protection of Critical Information Infrastructure [Electronic resource] // The State Council of People's Republic of China. [2021]. http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?mc_cid=da5881cf31&mc_eid=a268621911 (retrieved.: 14.11.2021)
13. Cybersecurity Act, B.E. 2562 (2019) [Electronic resource] // Office of the Council of State. [2021]. URL: http://web.krisdika.go.th/data/document/ext843/843708_0001.pdf (retrieved: 14.11.2021)
14. Personal Data Protection Act, B.E. 2562 (2019) [Electronic resource] // thainetizen.org. [2021]. URL: <https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf> (retrieved 14.11.2021).
15. Payment Systems Act, B.E. 2560 (2017) [Electronic resource] // web.krisdika.go.th. [2021]. URL: http://web.krisdika.go.th/data/document/ext810/810271_0001.pdf (retrieved: 14.11.2021)

References

1. e-Conomy SEA Spotlight 2020. At full velocity: Resilient and racing ahead [Electronic resource]. Google e-Conomy SEA 2020. [2021]. URL: <https://economysea.withgoogle.com/#explore> (retrieved: 14.11.2021)
2. Lockett H. Chinese tech stocks fall sharply on rising regulatory concerns [Electronic resource]. Financial Times. [2021]. URL: <https://www.ft.com/content/7bacf9ef-4ba0-4d5f-a471-144432847f57> (retrieved: 14.11.2021)
3. Toomgum S. Thailand among top 20 nations focusing on cybersecurity [Electronic resource]. The Nation. [2017]. URL: <http://www.nationmultimedia.com/detail/Economy/30325029> (retrieved: 14.11.2021)
4. Goryan E.V. Vedushchaya rol' Singapura v obespechenii kiberbezopasnosti v ASEAN: promezhutochnye rezultaty i perspektivy dal'nejshego rasshireniya. Territoriya novyh vozmozhnostej. Vestnik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa. 2018. Т. 10. № 3. S. 103 – 117.
5. IMD World Digital Competitiveness Ranking 2020 [Electronic resource]. IMD World Competitiveness Center. [2021]. URL: <https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/> (retrieved: 14.11.2021).
6. Belyaeva G.S. Pravovoj rezhim: k opredeleniyu ponyatiya. Istoricheskie, filosofskie, politicheskie i yuridicheskie nauki, kul'turologiya i iskusstvovedenie: Voprosy teorii i praktiki. 2012. Т. 17. № 3. CH. 2. S. 33 – 35.

7. Sergeeva E.I. YUridicheskie garantii v sisteme garantij prav lichnosti v Rossijskoj Federacii. *Zakon. Pravo. Gosudarstvo*. 2019. № 2 (22). S. 22 – 26.

8. Goryan E.V. Institucional'nye mekhanizmy obespecheniya bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i Singapura: sravnitel'no-pravovoj aspect. *Administrativnoe i municipal'noe pravo*. 2018. № 9. S. 49 – 60.

9. Goryan E.V. Rol' finansovogo reguljatora v obespechenii kiberbezopasnosti v Rossii i Singapure: sravnitel'no-pravovoj aspect. *Territoriya novyh vozmozhnostej. Vestnik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa*. 2019. T. 11. № 2. S.83 – 101.

10. 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.

11. Cybersecurity Law of the People's Republic of China [Electronic resource] // pkulaw.com. [2021]. URL: https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html (retrieved: 14.11.2021)

12. The Regulations on the Security and Protection of Critical Information Infrastructure [Electronic re-source]. The State Council of People's Republic of China. [2021]. http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?mc_cid=da5881cf31&mc_eid=a268621911 (retrieved.: 14.11.2021)

13. Cybersecurity Act, B.E. 2562 (2019) [Electronic resource] // Office of the Council of State. [2021]. URL: http://web.krisdika.go.th/data/document/ext843/843708_0001.pdf (retrieved: 14.11.2021)

14. Personal Data Protection Act, B.E. 2562 (2019) [Electronic resource] // thainetizen.org. [2021]. URL: <https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf> (re-trieved 14.11.2021).

15. Payment Systems Act, B.E. 2560 (2017) [Electronic resource] // web.krisdika.go.th. [2021]. URL: http://web.krisdika.go.th/data/document/ext810/810271_0001.pdf (retrieved: 14.11.2021)