Оригинальная статья / Original article

УДК 340

https://doi.org/10.21869/2223-1501-2025-15-1-29-38

О некоторых вопросах правового обеспечения информационной безопасности государства в современных условиях

С.Ю. Чапчиков[1] ✉

[1] Юго-Западный государственный университет
ул. 50 лет Октября, д. 94, г. Курск 305040, Российская Федерация

✉e-mail: tgpkstu@yandex.ru

Резюме

Актуальность. *Выделение на законодательном уровне информационной безопасности государства как нового национального приоритета требует совершенствования его правового обеспечения. Только разработка комплексной правовой платформы от базовых федеральных правовых актов до детализированных правовых актов регуляторов создаст эффективные условия для реализации данного стратегического национального приоритета Российской Федерации. Особенности и специфика данного приоритета должны быть в обязательном порядке учтены и при разработке регулирующих его правовых актов.*

Цель исследования *– определить механизмы повышения эффективности правового регулирования сферы информационной безопасности Российской Федерации.*

Задачи*: изучить содержание основных нормативных правовых актов в сфере обеспечения информационной безопасности в России; проанализировать состояние отечественного правового обеспечения информационной безопасности; оценить возможность повышения эффективности правового обеспечения информационной защищённости основ российской государственности.*

Методология. *При написании работы использовались методы анализа и синтеза, общенаучные (логические) приемы и инструментарий системного подхода.*

Результаты. *В ходе исследования установлено, что без должного правового обеспечения невозможно гарантировать реализацию нового национального приоритета – информационной безопасности Российской Федерации. Обоснована необходимость принятия мер по повышению эффективности правового регулирования данной сферы отношений.*

Вывод. *Для эффективного развития, функционирования и обеспечения безопасности отечественных цифровых платформ необходимо определение законодателем чётких дефиниций основных (ключевых) понятий в сфере информационной безопасности, что является основополагающим началом к разработке комплексной правовой базы данной сферы. Также необходима дополнительная проработка федеральными регуляторами (ФСБ России, ФСТЭК России) действующих правовых актов в этой сфере с целью их оптимизации путём детальной регламентации.*

Ключевые слова: *информационная безопасность; цифровизация; правовое обеспечение; правовое регулирование; защита информации; правовая база; федеральный регулятор.*

Конфликт интересов*: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Чапчиков С.Ю. О некоторых вопросах правового обеспечения информационной безопасности государства в современных условиях // Известия Юго-Западного государственного университета. Серия: История и право. 2025. Т. 15, № 1. С. 29–38. https://doi.org/10.21869/2223-1501-2025-15-1-29-38.

Поступила в редакцию 26.12.2024 Принята к публикации 24.01.2025 Опубликована 26.02.2025

On some issues of legal provision of information security of the state in modern conditions

Sergey Yu. Chapchikov[1] ✉

[1] Southwest State University
50 let Oktyabrya Str. 94, Kursk 305040, Russian Federation

✉ e-mail: tgpkstu@yandex.ru

Abstract

Relevance. *Highlighting the information security of the state at the legislative level as a new national priority requires improving its legal support. Only the development of a comprehensive legal platform from basic federal legal acts to detailed regulatory legal acts will create effective conditions for the implementation of this strategic national priority of the Russian Federation. The features and specifics of this priority must necessarily be taken into account when developing its regulatory legal acts.*

The purpose *of the study is to identify mechanisms for improving the effectiveness of legal regulation in the field of information security in the Russian Federation.*

Objectives: *to study the content of the main regulatory legal acts in the field of information security in Russia; to analyze the state of domestic legal support for information security; to assess the possibility of increasing the effectiveness of legal support for information security of the foundations of Russian statehood.*

Methodology. *When writing the work, methods of analysis and synthesis, general scientific (logical) techniques and tools of a systematic approach were used.*

The results *of the study. The study found that without proper legal support, it is impossible to guarantee the implementation of a new national priority – the information security of the Russian Federation. The necessity of taking measures to improve the effectiveness of legal regulation of this sphere of relations is substantiated.*

Conclusion. *For the effective development, functioning and security of domestic digital platforms, it is necessary for the legislator to define clear definitions of the main (key) concepts in the field of information security, which is only a fundamental beginning to the development of a comprehensive legal framework in this area. It is also necessary for the federal regulators (FSB of Russia, FSTEC of Russia) to further study the existing legal acts in this area in order to optimize them through detailed regulation.*

Keywords: *information security; digitalization; legal support; legal regulation; information protection; legal framework; information system operator; federal regulator.*

Conflict of interest: *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Chapchikov S.Yu. On some issues of legal provision of information security of the state in modern conditions. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2025;15(1):29–38. (In Russ.) https://doi.org/10.21869/2223-1501-2025-15-1-29-38.

Received 26.12.2024 Accepted 24.01.2025 Published 26.02.2025

***

Введение

Национальная безопасность Российской Федерации определяется как состояние защищённости национальных интересов от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойное качество их жизни, гражданский мир в государстве, охрана суверенитета Российской Федерации, её независимости и государственной целостности, социально-экономическое развитие страны.

Обновлённая Стратегия национальной безопасности Российской Федерации, утверждённая Указом Президента Российской Федерации от 2 июля 2021 г. № 400 (далее – Стратегия), впервые объ-

явила информационную безопасность (далее – ИБ) государства как новый национальный приоритет[1]. Это базовый документ стратегического планирования, определяющий национальные интересы и стратегические национальные приоритеты Российской Федерации, цели, задачи государственной политики в области обеспечения национальной безопасности и устойчивого развития Российской Федерации на долгосрочную перспективу [1]. В предыдущей версии Стратегии национальной безопасности России, которая была опубликована в конце 2015 г., ИБ не выделялась в отдельное направление, а входила в приоритет «наука, технологии и образование»[2].

По мнению секретаря Совета безопасности Российской Федерации Н.П. Патрушева (на момент утверждения обновлённой стратегии), выделение ИБ в качестве нового приоритета национальной безопасности вызвано более активным проявлением угроз на данном направлении. Такая приоритезация ИБ информресурсов государства призвана обеспечить суверенитет страны в информационном пространстве[3].

Кроме того, ряд значимых событий, произошедших в России и мире после принятия обновлённой Стратегии национальной безопасности Российской Федерации, кратно усилил проявление этого вида угроз в период 2022–2025 гг. К сожалению, эта тенденция сохраняется и на дальнейшую перспективу.

Цель исследования – определить механизмы повышения эффективности правового регулирования сферы информационной безопасности Российской Федерации.

Методология

При написании работы использовались методы анализа и синтеза, общенаучные (логические) приемы и инструментарий системного подхода. Методы анализа и синтеза позволили установить возрастающую значимость информационной безопасности в современных условиях и определить некоторые пути по её в том числе и правовому обеспечению. Общенаучные (логические) приемы и инструментарий системного подхода применялись для формулирования выводов по результатам исследования.

Результаты и их обсуждение

Качественное и количественное усиление угроз в сфере информационной безопасности требует комплексного подхода по выработке мер, направленных на их нейтрализацию [2]. Основополагающую роль в этом комплексе мер, несомненно, должен играть правовой блок. Несмотря на прошествие определённого периода времени с момента принятия обновлённой стратегии, остаётся много вопросов по развитию и совершенствованию правового регулирования в данной сфере, в том числе в научном мире [3].

Цифровизация есть внедрение современных цифровых технологий в различные сферы жизни и производства; в глобальном плане она, как отмечают многие современные исследователи, является концепцией экономической деятельности, основанной на цифровых технологиях, внедряемых в разные сферы жизни и производства [4, с. 85]. Это не только источник долгосрочного экономического роста страны и инструмент экономической гонки на мировой арене

[1] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 2 июля 2021 г. № 400 // Президент России: сайт. URL: https://www.kremlin.ru/acts/bank/47046 (дата обращения: 15.12.2024).

[2] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31 дек. 2015 г. № 683 // КонсультантПлюс: сайт. URL: https:// www.consultant.ru/document/cons_doc_LAW_191669/ (дата обращения: 10.12.2024).

[3] Секретарь Совбеза назвал главные для РФ угрозы кибербезопасности // D.Russia.Ru: сайт. URL: https://d-russia.ru/sekretar-sovbeza-nazval-glavnye-dlja-rf-ugrozy-kiberbezopasnosti.html (дата обращения: 10.12.2024).

(например, посредством повышения конкурентоспособности на рынке товаров и услуг, уровня жизни населения и т. д.), но и неотъемлемая составляющая суверенитета государства, его национальной безопасности [5].

Цифровизация является одной из главных современных целей и практических задач по развитию России. Это справедливо определяют многие современные учёные [6, с. 21]. Государство активно стимулирует регионы и компании переходить на цифровые рельсы, процесс затрагивает все сферы – от образования до строительства. В 2020 г. курс на цифровизацию закрепили на законодательном уровне Указом Президента Российской Федерации № 474 «О национальных целях развития Российской Федерации на период до 2030 года»[1]. По данным Минцифры Российской Федерации на ноябрь 2022 г., Россия вошла в ТОП-10 стран по цифровизации. В 2024 г. валовые внутренние затраты на развитие цифровой экономики в России составили 5,2 трлн руб. (+6,3% к 2021 г.). Почти две трети их объема формируют организации (+8,5%), треть – домашние хозяйства (+2,7%) [7, с. 125].

В основе определения принципов и механизмов развития цифровой экономики и цифровой трансформации находится концепция цифровой платформы.

Эксперты и законодатели в настоящее время не пришли к единому мнению в определении понятия «цифровая платформа». Это явление может рассматриваться с разных точек зрения: технологической, инфраструктурной, социальной, коммуникационной, экономической, финансовой, юридической[2]. Вот несколько вариантов описания того, что такое цифровая платформа [8].

1. «Система средств, поддерживающая использование цифровых процессов, ресурсов и сервисов значительным количеством субъектов цифровой экосистемы и обеспечивающая возможность их бесшовного взаимодействия» [9, с. 250].

2. «Бизнес по организации взаимодействия внешних производителей и потребителей, которое порождает для них новую ценность. Платформа предлагает открытую, совместно используемую инфраструктуру такого взаимодействия и устанавливает управляющие условия для участников» [10].

Однако не надо забывать, что цифровая трансформация – это не только комплексная программа внедрения современных цифровых технологий в процессы организации, она также подразумевает под собой преобразование всей структуры организации, общества, изменения концепций, а также способа и формата предоставления услуг, сервисов и продуктов. При этом некомплексный подход к переходу на цифровые рельсы открывает новые и довольно масштабные возможности для злоумышленников [11]. В эпоху геополитической нестабильности обеспечение цифровой (информационной) безопасности встает чуть ли не на первый план при реализации любого проекта, влияет в конце концов на национальную безопасность страны. Критически важно обращать внимание на данный аспект при внедрении новых цифровых решений, аппаратного и программного обеспечения.

Сегодня обеспечение информационной безопасности необходимо для защиты данных, хранящихся и обрабатывающихся на ресурсах организаций, ведомств, а также всех цифровых процессов. Только такой подход к реализации

[1] О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 21 июля 2020 г. № 474 // Президент России: сайт. URL: http://www.kremlin.ru/acts/bank/45726 (дата обращения: 14.12.2024).

[2] Технологии цифровизации в России – настала эпоха перемен. Что такое цифровизация и какие сферы жизни она заденет // Компания «Центр2М»: сайт. URL: https://center2m.ru/digitalization-technologies (дата обращения: 14.12.2024).

стратегии может обеспечить успех трансформации на каждом ее этапе [12]. Первостепенные задачи – внедрение методов и политик, направленных на предотвращение нежелательного доступа, обнаружение нарушений и успешное и своевременное реагирование на инциденты безопасности. Сетевая безопасность, безопасность конечных точек, шифрование данных, контроль доступа, планы реагирования на инциденты и обучение сотрудников, а также общее повышение осведомленности пользователей систем и приложений – одни из компонентов комплексного подхода к построению архитектуры кибербезопасности.

При всем разнообразии трактовок термина «цифровая платформа» представляется, что с точки зрения информационной безопасности наиболее удобно рассматривать её как информационную систему (далее – ИС) особого класса, которая позволяет неограниченному либо условно неограниченному кругу лиц пользоваться её возможностями через открытые телекоммуникационные сети (сеть Интернет) и решать свои технологические или функциональные задачи в автоматизированном режиме. В этом её существенное отличие от других информационных систем, в частности от внутренней информационной системы, пусть даже распределённой [13].

Такой подход к рассмотрению защищённости цифровых платформ удобен и с той точки зрения, что в настоящее время требования к защите информации в информационных системах достаточно чётко определены государством в соответствующих законах, постановлениях Правительства, нормативных правовых актах, стандартах, регламентах. В государстве создана система, позволяющая осуществлять контроль в этой области, выработаны единые требования к защите самих систем, средствам защиты информации, порядку подтверждения соответствия (аттестации по требованиям безопасности информации). Этот подход удобен ещё и тем, что к числу цифровых платформ относятся и государственные информационные системы (далее – ГИС), создаваемые в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях[1].

Число ГИС, их функции, задачи увеличиваются с каждым днём, растёт количество участников и пользователей, расширяется география их применения. Также растёт количество и ценность информации, обрабатываемой в ГИС. Следует напомнить, что под обработкой информации понимаются не только какие-либо операции над ней, но и прием, передача, хранение и уничтожение. Все это приводит к тому, что количество попыток несанкционированного доступа к этой информации с целью получения, искажения, запрета разрешённого доступа, неуклонно растет, множатся методы и способы взлома системы защиты [14].

Анализируя по роду деятельности архитектуру построения таких систем, имеющих в своем составе также и соответствующую систему защиты информации, все необходимые атрибуты и прошедшие процедуру независимой оценки соответствия системы требованиям руководящих документов по защите информации, можно выделить два характерных типа ИС.

Информационные системы первого типа, имея распределённую структуру, осуществляют взаимодействие между элементами системы (так называемое межсетевое взаимодействие) напрямую, используя в качестве каналов передачи данных или среду Интернет, или некие физические каналы (оптоволокно или

[1] Обеспечение безопасности информационных систем / Н. Махутов, В. Балановский, В. Подъяконов [и др.] // Системы безопасности: сайт. 2021. 11 окт. URL: https://www.secuteck.ru/articles/obespechenie-bezopasnosti-informa-cionnyh-sistem (дата обращения: 11.11.2024).

медь). Разумеется, между элементами системы организован на базе существующего физического канала свой, защищенный, использующий сертифицированные криптографические средства.

В свою очередь, информационные системы второго типа, также распределенные, имеют несколько другое построение. При прочих равных условиях с системами первого типа у них организовано межсетевое взаимодействие с использованием промежуточных звеньев в виде других информационных систем, пусть даже имеющих соответствующие документы, подтверждающие соответствие информационной системы требованиям безопасности информации.

В пользу построения межсетевого взаимодействия по второму типу главным аргументом является прежде всего снижение себестоимости системы защиты информации для конечного пользователя (абонента), уменьшение его финансовой нагрузки. Также приводятся аргументы в пользу этого решения в виде стойкого криптоалгоритма, сертифицированных средств защиты информации. И такая схема нашла многих сторонников. В рамках данной статьи мы не будем оценивать юридическую и техническую сторону этого решения. Для краткости лишь заметим, что для первого случая четко определены границы ответственности должностных лиц в случае несанкционированного доступа и возникновения негативных последствий для государства и личности. Во втором случае границы ответственности становятся размытыми, и эта неопределенность увеличивается с ростом промежуточных межсетевых взаимодействий. Это с точки зрения юриспруденции. С технической точки зрения приведем лишь один довод, не требующий сложных математических вычислений.

Известно, что скорость передачи информации определяется в том числе и следующими факторами: техническими характеристиками передающего и приемного оборудования, пропускной способностью канала передачи данных, его длиной, количеством промежуточных узлов телекоммуникационного оборудования. Естественно, при каскадном межсетевом взаимодействии количество узлов телекоммуникационного и иного оборудования будет только возрастать, что неминуемо приведёт к снижению пропускной способности и производительности (не будем забывать и о необходимости криптографической защиты).

Более подробно хотелось бы остановиться на анализе выполнения требований руководящих документов по защите информации в случае использования промежуточных информационных систем при взаимодействии элементов ГИС.

В качестве источника этих требований воспользуемся одним из основополагающих документов: Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17 (далее – Требования)[1]. В документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях её добывания, уничтожения, искажения или блокирования доступа к ней (далее – защита информации) при обработке указанной информации в государственных информационных системах.

[1] Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февр. 2013 г. № 17: посл. ред. // Консультант Плюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_147084/ (дата обращения: 10.12.2024).

Документ также определяет перечень обязательных мероприятий для обеспечения защиты информации:

– формирование требований к защите информации, содержащейся в информационной системе;

– разработка системы защиты информации информационной системы;

– внедрение системы защиты информации информационной системы;

– аттестация информационной системы по требованиям защиты информации (далее – аттестация информационной системы) и ввод её в действие;

– обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

– обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Первый этап, этап формирования требований к защите информации, является, по нашему мнению, самым важным, определяет качество и достаточность всех дальнейших мероприятий. Наряду с целями и задачами обработки информации на первом этапе определяется значимость обрабатываемой информации, ее объем, что в дальнейшем позволяет сформировать конкретный перечень мер, обеспечивающих ее защиту.

Однако основополагающим документом на данном этапе является так называемая модель угроз безопасности информации, в которой производится оценка возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности). При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

При моделировании угроз для информационной системы, построенной по первой схеме, картина представляется достаточно ясной, прогнозируемой. В ней можно четко выделить типы возможных нарушителей (внутренние, внешние), определить перечень угроз, предусмотреть в дальнейшем возможность модернизации системы защиты в случае масштабирования. Во втором случае при использовании для связи и защищенного взаимодействия элементов другой информационной системы картина меняется, возникает неоднозначность, которая в дальнейшем может привести к нежелательным последствиям.

Известно, что для защищенности информационной системы наиболее опасными нарушителями является так называемый внутренний нарушитель. По статистике, более 70% всех инцидентов безопасности приходится на внутреннего нарушителя. И защита от них представляется наиболее сложной, т. к. он обладает максимальными возможностями по доступу к элементам системы и обладает наиболее достоверными знаниями о структуре самой системы и способах защиты. Критерий отнесения нарушителя к внутреннему типу достаточно прост – он должен находиться внутри контролируемой зоны информационной системы [15].

Рассматривая топологию системы, применить данный критерий просто и понятно. В случае же построения информационной системы по второму типу по-

тенциальный нарушитель промежуточной системы, являясь внешним по отношению к нашей системе, по своим возможностям воздействия на элементы межсетевого взаимодействия является наиболее опасным, внутренним. И что самое главное, при моделировании угроз мы не можем определить его возможности, спрогнозировать его действия. Поэтому мы вынуждены для исключения нарушения свойств безопасности информации предполагать его самые изощрённые возможности и использовать самые стойкие криптографические средства, что приводит к усложнению и удорожанию системы защиты.

Но использование стойких криптографических средств защищает конфиденциальность и целостность информации. Проблему доступности информации средства криптографии не снимают. И если в первом случае при нарушении канала связи мы можем воспользоваться альтернативным каналом, то во втором случае эта возможность отсутствует, т. к. межсетевое взаимодействие предполагает жесткие ограничения по маршруту, в том числе и аппаратные.

При построении информационной системы с использованием межсетевого взаимодействия возникают вопросы и при выполнении дальнейших мероприятий, определённых документом при создании системы защиты информации.

Особую озабоченность вызывает и выполнение мероприятий по защите информации в ходе эксплуатации информационной системы, этапа жизненного цикла наиболее важного и продолжительного по времени.

Проецируя эти мероприятия на имеющийся опыт проектирования и создания систем защиты информации, нам представляется, что их реализация в случае межсетевого взаимодействия будет затруднена, а в некоторых случаях и невозможна.

Выводы

Таким образом, для эффективного развития, функционирования и обеспечения безопасности отечественных цифровых платформ необходимо определение законодателем чётких дефиниций основных (ключевых) понятий в сфере информационной безопасности, что является основополагающим началом в разработке комплексной правовой базы данной сферы. Кроме того, необходима дополнительная проработка федеральными регуляторами (ФСБ России, ФСТЭК России) действующих правовых актов с целью их оптимизации путём детальной регламентации деятельности операторов государственных и негосударственных информационных систем, направленной на минимизацию рисков в сфере информационной безопасности и упрощения задач по выявлению и борьбе с ними.

Список литературы

1. Казанцев С.В. О стратегии экономической безопасности // Мир новой экономики. 2016. № 3. С. 6–13.

2. Клепач А.Н. Международные санкции и ответные меры: возможен ли позитив для российской экономики? Заседание диспут-клуба Ассоциации независимых центров экономического анализа // Мир новой экономики. 2015. № 1. С. 6–12.

3. Сильвестров С.Н. Выбор в условиях глобальной неопределенности // Мир новой экономики. 2015. № 2. С. 6–19.

4. Моргунов Е.В., Жуковская Л.В. Рента как основа государственных финансов // Доходы, расходы и сбережения населения России: тенденции и перспективы: сборник материалов II Всероссийской научно-практической конференции. М.: Акварель, 2016. С. 60–62.

5. Моргунов Е.В., Мамаев С.М. Развитие городов через призму качества жизни населения // Вестник Томского государственного университета. Экономика. 2017. № 38. С. 26–42.

6. Моргунов Е.В., Мигранова Л.А., Мамаев С.М. Уровень и качество жизни городского населения (итоговый отчет): Исследование развития городов через призму уровня и качества жизни населения. М.: ИСЭПН РАН, 2016. 30 с.

7. Моргунов Е.В., Томилина Е.Е. Фонд будущих поколений как правовой институт трансформации рентных доходов (на примере постоянного фонда Аляски) // Право и юридическая реализация / под ред. С.Г. Киселева. М.: МАКС Пресс, 2015. 332 с.

8. Моргунов Е.В., Чернявский С.В. Политика национального интереса как альтернатива либерализму // Управление. 2014. № 3. С. 57–61.

9. Народонаселение современной России: воспроизводство и развитие / под ред. проф. В.В. Локосова. М.: Экон-Информ, 2015. 411 с.

10. Чернявский С.В. Критика «сверхприбыльной концепции» природно-ресурсной ренты // Вестник университета (Государственный университет управления). 2012. № 18. С. 102–105.

11. Чернявский С.В. Недостатки использования НДПИ с плоской шкалой и направления его совершенствования // Вестник Томского государственного университета. 2013. № 370. С. 136–139.

12. Шинкарецкая Г.Г., Берман А.М. Цифровизация и проблема обеспечения национальной безопасности // Образование и право. 2020. № 5. С. 254–260.

13. Корабельников С.М. Цифровизация и национальная безопасность // Вестник Российской правовой академии. 2022. № 1. С. 44–49.

14. Полякова Т.А. Базовые принципы правового обеспечения информационной безопасности // Труды Института государства и права РАН. 2016. № 3 (55). С. 17–40.

15. Шинкарецкая Г.Г. Цифровизация – глобальный тренд мировой экономики // Образование и право. 2019. № 8. С. 119–123.

References

1. Kazancev S.V. On the strategy of economic security. *Mir novoi iekonomiki = The world of the new economy*. 2016;(3):6–13. (In Russ.)

2. Klepach A. N. International sanctions and retaliatory measures: is a positive for the Russian economy possible? Meeting of the dispute Club of the Association of Independent Centers of Economic Analysis. *Mir novoi iekonomiki = The world of the new economy*. 2015;(1):6–12. (In Russ.)

3. Sil'vestrov S.N. Choice in conditions of global uncertainty. *Mir novoi iekonomiki = The world of the new economy.* 2015;(2):6–19. (In Russ.)

4. Morgunov E.V., Zhukovskaja L.V. Rent as the basis of public finance. In: Lokosov V.V. (ed.) *Dohody, rashody i sberezhenija naselenija Rossii: tendencii i perspektivy: sbornik materialov II Vserossijskoj nauchno-prakticheskoj konferencii = Incomes, expenses and savings of the Russian population: trends and prospects: collection of materials of the II All-Russian Scientific and Practical Conference*. Moscow: Akvarel'; 2016. P. 60–60. (In Russ.)

5. Morgunov E.V., Mamaev S.M. Development of cities through the prism of the quality of life of the population. *Vestnik Tomskogo gosudarstvennogo universiteta. Ekonomika = Bulletin of Tomsk State University. Economy*. 2017;(38):6–42. (In Russ.)

6. Morgunov E.V., Migranova L.A., Mamaev S.M. The level and quality of life of the urban population (final report): A study of urban development through the prism of the level and quality of life of the population. Moscow: ISJEPN RAN; 2016. 30 p. (In Russ.)

7. Morgunov E.V., Tomilina E.E. The Fund of future generations as a legal institution for the transformation of rental income (on the example of the permanent fund of Alaska). *Pravo i yuridicheskaya realizaciya = Law and legal implementation*. Moscow: MAKS Press; 2015. 332 p. (In Russ.)

8. Morgunov E.V., Chernyavskij S.V. Politics of national interest as an alternative to liberalism. *Upravlenie = Management*. 2014;(3):57–61. (In Russ.)

9. Lokosova V.V. (ed.) Population of modern Russia: reproduction and development. Moscow: Ekon-Inform; 2015. 411 p. (In Russ.)

10. Chernyavskij S.V. Criticism of the "super-profitable concept" of natural resource rent. *Vestnik universiteta (Gosudarstvennyj universitet upravleniya) = Bulletin of the University (State University of Management)*. 2012;(18):102–105. (In Russ.)

11. Chernyavskij S.V. Disadvantages of using MET with a flat scale and directions for its improvement. *Vestnik Tomskogo gosudarstvennogo universiteta = Bulletin of Tomsk State University*. 2013;(370):136–139. (In Russ.)

12. Shinkareckaya G.G., Berman A.M. Digitalization and the problem of ensuring national security. *Obrazovanie i pravo = Education and law*. 2020;(5):254–260. (In Russ.)

13. Korabel'nikov S.M. Digitalization and national security. *Vestnik Rossiiskoi pravovoi akademii = Bulletin of the Russian Law Academy*. 2022;(1):44–49. (In Russ.)

14. Polyakova T.A. Basic principles of legal support for information security. *Trudy Instituta gosudarstva i prava RAN = Proceedings of the Institute of State and Law of the RAS*. 2016;(3):17–40. (In Russ.)

15. Shinkareckaya G.G. Digitalization – a global trend in the world economy. *Obrazovanie i pravo = Education and Law*. 2019;(8):119–123. (In Russ.)

Информация об авторе / Information about the Author

Чапчиков Сергей Юрьевич, доктор юридических наук, профессор кафедры теории и истории государства и права, Юго-Западный государственный университет, г. Курск, Российская Федерация,
e-mail: tgpkstu@yandex.ru,
ORCID: 0009-0008-1785-1019

Sergey Y. Chapchikov, Doctor of Sciences (Juridical), Lecturer of Departments of Theory and History of State and Law, Southwest State University, Kursk, Russian Federation,
e-mail: tgpkstu@yandex.ru,
ORCID: 0009-0008-1785-1019