УДК 340.5

DOI: https://doi.org/10.17816/RJLS106912

Правовые механизмы защиты цифрового суверенитета государства: сравнительно-правовой аспект

Д.А. Печегин

Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, Москва, Россия

Аннотация. Стремительное развитие цифровых технологий, ставшее отличительной особенностью современности, определяет векторы эволюции общественных отношений и обусловливает модификации их регуляторов, в числе которых ключевое значение отводится как технологиям, так и праву. Транспорт, экономика, производство, энергетика, сельское хозяйство, образование, здравоохранение, финансы — вот лишь некоторые сферы, которые, являясь ключевыми для современного общества и государства, подвержены цифровой трансформации. Причины столь масштабного проникновения цифровых технологий в среду *jus publicum* усматриваются в эффективности инструментария, используемого для достижения поставленных целей. Большие данные, машинное обучение, нейронные сети, искусственный интеллект, виртуальная реальность, интернет вещей, роботизация и другие инструменты цифровизации позволяют достигнуть такой автоматизации в обозначенных сферах, при которой в конкретный момент получения, обработки и анализа данных с уверенностью прогнозируется текущее состояние на рынке. Это позволяет в сжатые сроки предопределить выбор наиболее эффективной модели поведения и максимизировать прибыль, особенно в бизнес-среде. Иными словами, именно цифровые технологии сегодня становятся основой поддержки конкурентоспособности, причем не только бизнес-сообщества, но, прежде всего, государства. Однако проблема состоит в том, что в основу цифровизации отмеченных общественных отношений, охватываемых *jus publicum*, и государственности сегодня положены решения и алгоритмы, которые не только разработаны и внедрены в практику **частными** компаниями, но, прежде всего, предполагают построение сервис-ориентированной архитектуры отношений, исключающей самостоятельность (цельность, завершенность) любого цифрового продукта (товара, услуги). В таких условиях значительно возрастают риски утраты независимости и верховенства власти государства, если отсутствуют какие-либо альтернативы. Статья посвящена анализу правовых механизмов защиты **(цифрового)** суверенитета в сравнительно-правовом аспекте.

Ключевые слова: суверенитет; цифровой суверенитет; Big Data; искусственный интеллект; продукт-сервис; алгоритмы; цифровизация; цифровые технологии; верховенство власти государства в условиях цифровизации.

Как цитировать:
Печегин Д.А. Правовые механизмы защиты цифрового суверенитета государства: сравнительно-правовой аспект // Российский журнал правовых исследований. 2022. Т. 9. № 2. С. 9–20. DOI: https://doi.org/10.17816/RJLS106912

Рукопись получена: 28.04.2022 **Рукопись одобрена:** 08.05.2022 **Опубликована:** 30.06.2022

DOI: https://doi.org/10.17816/RJLS106912

Legal Mechanisms for the Protection of State Digital Sovereignty: a Comparative Legal Aspect

D.A. Pechegin

The Institute of legislation and comparative law under the government of the Russian Federation, Moscow, Russia

ABSTRACT: The rapid development of digital technologies, which has become a distinctive feature of modernity, determines the vectors of the evolution of public relations and modifications of their regulators, among which both technology and law are critical. Transport, economy, manufacturing, energy, agriculture, education, healthcare, and finance are just some of the areas that, being keys for the development of modern society and the state, are subject to digital transformation. The large-scale penetration of digital technologies into the *jus publicum* environment is mainly owing to the effectiveness of the tools available to achieve the goals set. Digitalization tools, such as big data, machine learning, neural networks, artificial intelligence, virtual reality, the Internet of Things, and robotics, make it possible to achieve automation, such that the current state of the market is confidently predicted at the particular moment of receiving, processing, and analyzing the data. This allows a swift determination of the most effective behavior model and maximizes profits, especially in the business environment. Digital technologies are thus becoming the basis for supporting competitiveness today, not only for the business community, but more importantly, the state. However, the problem is that the digitalization of public relations covered by *jus publicum* and statehood today is based on solutions and algorithms that are developed and put into practice by **private** companies and involve the construction of service-oriented relationship architectures that exclude the independence (integrity, completeness) of the digital products (goods, services). Consequently, the risks of losing the independence and supremacy of state power increase significantly; hence, the need to find alternatives. This article is devoted to the analysis of legal mechanisms for the protection of (**digital**) sovereignty in a comparative legal aspect..

Keywords: sovereignty; digital sovereignty; big data; artificial intelligence; product-service; algorithms; digitalization; digital technologies; the supremacy of state power in the conditions of digitalization.

To cite this article:
Pechegin DA. Legal mechanisms for the protection of state digital sovereignty: a comparative legal aspect. *Russian journal of legal studies*. 2022;9(2):9–20. DOI: https://doi.org/10.17816/RJLS106912

Received: 28.04.2022 **Accepted:** 08.05.2022 **Published:** 30.06.2022

Все большее число традиционных функций государства подвергается технологизации, позволяющей обеспечить легкий доступ к услугам и ускорить получение искомого результата [1, с. 150], поскольку современные решения значительно расширяют возможности по сбору и обработке данных. Неслучайно в Доктрине информационной безопасности Российской Федерации отмечено, что «технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства»[1].

Например, согласно отчету Центрального Банка России «Основные направления развития технологий SupTech и RegTech на период 2021–2023 годов»[2] многие регуляторы и участники финансового рынка разработали и внедряют технологии и технологические стратегии, которые включают в себя не только содействие поднадзорным организациям в применении собственных или вендорских решений, но и их совместное принятие для упрощения и оптимизации выполнения регуляторных требований. При этом основными сферами применения технологий (как цифровых, так и сопутствующих им) являются мониторинг мошеннических действий, противодействие недобросовестным практикам и легализации (отмыванию) преступных доходов, в том числе денежных средств, преобразованных из виртуальных активов (криптовалют)[3].

Более того, цифровые права признаны объектами гражданских прав в соответствии со статьями 128 и 141[1] Гражданского кодекса Российской Федерации (некоторые исследователи относят нематериальные объекты, которые имеют экономическую ценность, полезны и могут быть использованы исключительно в виртуальном пространстве, к виртуальному имуществу [2]). Однако беспрецедентный характер технологий цифрового уровня (большие данные, машинное обучение, нейронные сети, искусственный интеллект, виртуальная реальность, интернет вещей, роботизация и др.) заключается в том, что они не только расширяют указанные возможности, но, по меньшей мере, позволяют с достоверностью спрогнозировать, в какой точке будет сформирована «максимальная добавочная стоимость, где начинаются и кончаются цепочки поставок, каковы пути их оптимизации, как живут люди, что они потребляют и как меняется потребление, в какие отрасли и проекты надо направить инвестиции для получения больших сравнительных преимуществ» [3], т.е. максимизировать прибыль и др. Кроме того, все большее число традиционных функций государства подвергается цифровой технологизации, позволяющей обеспечить легкий доступ к услугам и ускорить получение результата, все большее число секторов обеспечения жизни общества и функционирования государственных органов (образований) становятся самостоятельными объектами критической информационной инфраструктуры (далее — КИИ) Российской Федерации либо их составными элементами.

Тем не менее организация и правила функционирования цифровых технологий заведомо не адаптированы к действующему нормативному регулированию, что не позволяет в должной мере следовать правовым механизмам, которые предназначены для защиты публичного правопорядка. Более того, экстенсивный характер развития цифровых технологий и отсутствие надлежащей адаптации правового регулирования к обеспечению безопасности возникающих в новой среде отношений ставят под угрозу возможность эффективного противодействия актам противоправного поведения в цифровом пространстве, особенно в условиях дифференциации пространственного и цифрового развития в Российской Федерации [4, с. 296].

Однако главной проблемой остается импортная зависимость [5, с. 210–211]. Подавляющее большинство цифровых технологий в своей основе не содержат отечественных решений. Примечательно, что 75 % всех патентов по технологии блокчейн, 50 % мировых расходов на интернет вещей и более 75 % мирового рынка общедоступных облачных вычислений, а также 90 % рыночной капитализации 70 крупнейших мировых цифровых платформ распределены всего лишь между двумя государствами — США и Китаем, при этом данная проблема подвержена активной дискуссии в других государствах, в том числе входящих в состав ЕС [6, с. 29–30]. Это означает не что иное, как то, что даже в случае успешного построения цифровой экономики управление и регулирование ключевых секторов экономики, а также выработка механизмов обеспечения безопасности объектов КИИ в стратегическом отношении будут зависеть от избранных за рубежом направлений технологического совершенствования в широком смысле (включая преобразование исходных кодов, внедрение новых технологических и программных решений, обновление процессинга данных и др.).

По этим причинам в условиях стремительного развития и внедрения цифровых технологий ключевым аспектом становится обеспечение суверенитета государства в новых условиях [7, с. 206], по меньшей мере в контексте свода различных государственных программ и проектов технологической (цифровой) трансформации политического, экономического и культурного пространств в единое целое [8, с. 30]. Кратко рассмотрим наиболее значимые направления правовой защиты цифрового суверенитета за рубежом на примере юрисдикций (групп

[1] Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

[2] URL: http://www.cbr.ru/press/event/?id=9801 (дата обращения: 28.04.2022).

[3] Пункт 1 Постановления Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем».

юрисдикций), входящих в число лидеров по возможности развития цифровых технологий и их внедрению в правоприменительную практику.

1. Документы стратегического планирования

Стратегии и рекомендации представляют собой довольно распространенный инструмент при принятии теми или иными ведущими в технологическом отношении юрисдикциями согласованных решений в какой-либо сфере, в том числе цифровой. При этом, как правило, такие инструменты используются для целей формирования основ обеспечения безопасности конкретных отношений в цифровой среде, например, складывающихся в ходе обработки персональных данных, функционирования объектов КИИ, оборота цифровых активов.

В США с периодичностью в 4–5 лет разрабатывается стратегический план обеспечения национальной безопасности. Так, в настоящее время реализуется Стратегический план национальной безопасности США на 2020–2024 гг., в котором сформулированы цели и задачи Департамента общественной безопасности США (далее — DHS), а также стратегии, которые используются для достижения целей, и долгосрочные показатели эффективности. Как одно из ключевых направлений стратегического планирования выделяется обеспечение безопасных киберпространства и объектов КИИ. Выступая в качестве назначенного федерального лидера по кибербезопасности в правительстве США, DHS способствует принятию общих политик и передовых методов, основанных на оценке рисков и реагирующих на постоянно меняющуюся среду киберугроз, включая цифровые технологии. Кроме того, DHS сотрудничает с межведомственными партнерами для развертывания возможностей обнаружения вторжений, предотвращения несанкционированного доступа и создания отчетов о рисках кибербезопасности практически в режиме реального времени[4]. Согласно цели 4.4 «Защита финансовой системы США» экономическое процветание США поставлено в зависимость от глобального доверия к доллару США и надежным финансовым институтам и платежным системам как важнейшим элементам глобальной торговли. При этом несмотря на то обстоятельство, что «оцифровка» финансовых систем упростила торговлю и принесла пользу мировой экономике, она также подвергла финансовые операции новым векторам атак. Специально указано, что цифровые валюты создают новые проблемы для DHS по противодействию фальшивомонетничеству, поскольку закладывают рамки для расширения использования IT-достижений, чтобы идти в ногу со средой угроз, либо уделения приоритетного внимания расследованиям правоохранительных органов, которые противодействуют наиболее значительным криминальным угрозам в сотрудничестве с другими правоохранительными органами в рамках соответствующих полномочий[5]. Примечательно, что наряду с указанным планом аналогичные документы стратегического характера принимаются в контексте юрисдикции каждого штата.

В Китае политика в области обеспечения «киберсуверенитета» определила позицию страны в сферах управления данными и технологического развития. В рамках масштабной китайской инициативы «Один пояс — один путь» (далее — BRI), крупнейшего инфраструктурного проекта в мире, в 2015 г. был инициирован запуск проекта «Цифровой шелковый путь» (далее — DSR), в соответствии с которым Китай предоставляет помощь и политическую поддержку государствам-участникам. DSR также оказывает поддержку китайским экспортерам, в том числе многим известным китайским технологическим компаниям, таким как Huawei. Помощь DSR направлена на улучшение телекоммуникационных сетей получателей, возможностей искусственного интеллекта, облачных вычислений, систем электронной коммерции и мобильных платежей, технологий видеонаблюдения, умных городов и других высокотехнологичных областей. Центральное место в цифровой стратегии Китая при этом занимает ужесточение государственного контроля над цифровой сферой с точки зрения онлайн-контента, защиты данных и преференций для представителей национального бизнес-сообщества[6]. Правительство страны стремится выделить цифровое пространство Китая и ограничить власть субъектов частного сектора, как иностранных, так и внутренних.

В ЕС в 2015 г. была принята Стратегия единого цифрового рынка (Digital Single Market Strategy 2015), содержащая 16 инициатив по обеспечению доступа цифровых товаров и услуг на территории государств — членов ЕС. Соответствующие инициативы (например, образование европейских платформ электронной коммерции) предполагают создание на территории ЕС единого рынка цифровых товаров и услуг, для целей максимизации роста которого конкретные страны должны принять регуляторные решения, обеспечивающие наиболее подходящие условия развития цифровых отношений в ЕС. В 2016 г. на уровне ЕС также был принят Генеральный регламент о защите данных (*General Data Protection Regulation*), направленный на унификацию порядка обработки данных. Согласно условиям данного регламента, любая организация, независимо от того, где она базируется, должна соблюдать набор правил управления данными, если она хочет торговать с клиентами в странах ЕС. С учетом данных документов в 2021 г. в ЕС были кодифицированы детальные правила деятельности провайдеров облачных сервисов для защиты персональных данных (*the 2021 EU*

[4] URL: https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure (дата обращения: 27.04.2022).

[5] URL: https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf (дата обращения: 27.04.2022).

[6] Trace the Digital Silk Road projects, part of China's massive Belt and Road Initiative, around the world—and the effects of China's investments. URL: https://www.cfr.org/china-digital-silk-road/ (дата обращения: 27.04.2022).

Cloud Code of Conduct). Особенностью этого кодекса является то, что он — первый в мире высокоэффективный источник нормативных предписаний, которые обеспечивают соблюдение необходимых требований участниками, не будучи юридически обязательными. Тем не менее разрешение на использование облачных сервисов на внутреннем рынке ЕС предоставляется только компаниям, которые соблюдают требования указанного кодекса. Примечательно, что такие компании, как Alibaba Cloud, Google Cloud, IBM и Microsoft, внедрили в свои системы положения о защите данных в соответствии требованиями этого акта[7].

Отдельно следует обратить внимание на цифровой вектор развития рекомендаций, направленных на формирование стратегических основ противодействия отмыванию денежных средств, полученных преступным путем с помощью цифровых валют и иных финансовых инструментов, выраженных в цифровой форме, которые неизбежным образом влияют на трансформацию правовых средств воздействия на охраняемые законом общественные отношения, например ФАТФ. Принимая соответствующие стандарты и рекомендации, ФАТФ осуществляет мониторинг их исполнения, проводит исследования рисков, трендов и типологий отмывания денег и финансирования терроризма с разработкой методологии борьбы с этими видами преступлений [9] и др. Так, операторы криптовалютных сервисов (в первую очередь, биржи криптовалют) обязаны передавать друг другу информацию о клиентах при совершении ими переводов средств между биржами. При этом информация должна передаваться не только о переводах в фиатных валютах, но и о криптовалютных транзакциях. Все операторы услуг, связанных с криптовалютами, обязаны получить лицензию регулятора в своей стране. ФАТФ также рекомендует использовать открытые источники информации, включая мониторинг Интернета и рекламных объявлений, для идентификации незарегистрированных или нелицензированных сервисов. Руководство рынка цифровых финансов касается и предотвращения использования криптовалютными сервисами методов сокрытия реальных отправителей и получателей транзакций, включая микшеры, тумблеры и анонимные криптовалюты. Сервисы, неспособные контролировать использование подобных приемов, могут быть закрыты регуляторами.

Эти и другие требования стратегического характера позволяют отдельным странам лучше контролировать то, как могут использоваться их данные и сведения об их гражданах, выстраивать конкурентоспособную цифровую среду, отвечающую требованиям национальной (наднациональной) безопасности. Так, в Германии с учетом отмеченных программных требований в ходе реализации исследования «Пути развития цифровой Германии 2020» были сформулированы основы для политико-правового обрамления мер по обеспечению ее цифрового суверенитета [10; 11, с. 147]. Более того, в 2019 г. Германия объявила инициативу под названием *Gaia-X* — прототип будущего европейского облачного провайдера, формируемый с целью создания «конкурентоспособной, безопасной и надежной» инфраструктуры передачи данных для ЕС[8], а в 2020 г. анонсировала намерение установить цифровой суверенитет в качестве лейтмотива европейской цифровой политики[9] на период 2020–2030 гг.

2. Регуляторные механизмы защиты цифрового суверенитета

С учетом изложенных политико-стратегических подходов к обеспечению национального (наднационального) цифрового суверенитета в США, Китае и ЕС принимаются конкретные законодательные акты, устанавливающие регуляторные механизмы их реализации.

В США меры обеспечения безопасности объектов КИИ регламентированы Законом о защите критической инфраструктуры (42 U.S. Code § 5195c - Critical infrastructures protection). Согласно данному акту термин «критическая инфраструктура» означает системы и активы, будь то физические или виртуальные, настолько жизненно важные для США, что выход из строя или разрушение таких систем и активов окажет пагубное воздействие на безопасность и (или) национальную экономическую безопасность, национальную общественность, здравоохранение.

Оценка указанных рисков в соответствии с подразделом «B» титула II «Критическая информационная инфраструктура» Закона о национальной безопасности 2002 года (Homeland Security Act of 2002) осуществляется специальным ведомством. При Агентстве США по кибербезопасности и безопасности инфраструктуры создан Национальный центр моделирования и анализа инфраструктуры (далее — NISAC), который является научно-исследовательским подразделением по анализу рисков, ориентированным на создание передовых аналитических инструментов, предоставляющих исчерпывающую, количественную и полезную информацию для улучшения понимания того, как управлять указанными рисками. NISAC осуществляет значительные и эффективные инвестиции в различные группы федеральных исследовательских центров для удовлетворения аналитических потребностей сообщества критической инфраструктуры и устранения возникающих межотраслевых рисков. В частности, участвует в разработке мер, необходимых для защиты ключевых ресурсов и объектов КИИ США, в том числе в координации с другими учреждениями федерального правительства и в сотрудничестве с государственными

[7] URL: https://www.swp-berlin.org/en/publication/advancing-european-internal-and-external-digital-sovereignty (дата обращения: 25.04.2022).

[8] URL: https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4 (дата обращения: 25.04.2022).

[9] URL: https://policyreview.info/concepts/digital-sovereignty (дата обращения: 25.04.2022).

и местными правительственными учреждениями и органами власти, частным сектором и другими организациями.

Более того, в Конгрессе США рассматривается законопроект о создании Национального фонда США по содействию киберустойчивости, расширении возможности федерального правительства по оказанию помощи в повышении киберустойчивости критической инфраструктуры, повышении безопасности национальной киберэкосистемы, решении проблемы системно важной критической инфраструктуры и для других целей (S.2491 - Defense of United States Infrastructure Act of 2021)[10]. Законопроект направлен на уменьшение уязвимостей объектов КИИ США посредством тесной кооперации государственного и частного секторов в вопросах обеспечения состояния киберзащищенности. Для этих целей в Казначействе США учреждается «Национальный фонд помощи в обеспечении киберустойчивости», который должен быть доступен для оплаты риска — программы грантов, направленных на систематическое повышение устойчивости государственной и частной критически важной инфраструктуры к рискам кибербезопасности, что должно повысить общую устойчивость США в киберпространстве.

Кроме того, согласно указанному законопроекту в США будут созданы не менее одного и не более трех центров безопасности критически важных технологий для выполнения: (i) тестирования безопасности сетевых технологий для проверки безопасности аппаратного и программного обеспечения, связанного с киберпространством; (ii) тестирования безопасности подключенной промышленной системы управления для проверки безопасности подключенных программируемых логических контроллеров данных, серверов диспетчерского управления и сбора данных и другого промышленного оборудования, подключенного к сети; и (iii) тестирования безопасности программного обеспечения с открытым исходным кодом для тестирования и координации усилий по устранению уязвимостей в программном обеспечении с открытым исходным кодом.

Регулирование финансово-цифровых отношений в США сосредоточено вокруг использования в гражданском обороте криптовалют. Еще в 2013 г. Бюро по борьбе с финансовыми преступлениями (FinCEN) опубликовало документ, в котором констатируется, что биржи и администраторы криптовалют подпадают под действие закона США о банковской тайне (Bank Secrecy Act of 1970, далее — BSA), направленного на противодействие легализации (отмыванию) денежных средств, и должны регистрироваться в качестве бизнеса, связанного с предоставлением денежных (платежных) услуг. В частности, BSA требует от финансовых учреждений вести учет покупок оборотных инструментов наличными, представлять отчеты, если сумма ежедневных платежей превышает 10 000 долларов США, и сообщать о подозрительной деятельности, которая может свидетельствовать об отмывании денег и другой преступной деятельности [12].

В настоящее время на рассмотрении Конгресса США находится законопроект о криптоактивах (H.R.6154 — Crypto-Currency Act of 2020)[11]. Проект разделяет все криптоактивы на три вида: 1) криптовалюты; 2) криптотовары; 3) криптобумаги (ценные бумаги). Каждый вид криптоактивов будет регулироваться в США тремя самостоятельными[12] государственными органами, которые обозначены применительно к новой криптосфере термином крипторегулятор (т.е. предполагается, что в США будет принято общее законодательство, в целом относящееся к деятельности криптрегуляторов, а также самостоятельное регулирование криптрегуляторами «своего» криптоактива). Так, криптовалюты отнесены к ведению FinCEN, криптотовары — к Commodity Futures Trading Commission (CTFC), криптобумаги — к Комиссии по ценным бумагам и биржам (SEC). Каждый криптрегулятор обязан предоставлять общественности и поддерживать в актуальном состоянии список всех федеральных лицензий, сертификатов или регистраций, необходимых для создания или торговли криптоактивами. Кроме того, Казначейство США в лице его Секретаря и через FinCEN будет обязано установить правила, аналогичные финансовым учреждениям, о возможности отслеживать транзакции криптовалюты.

Подход Китая к цифровому суверенитету законодательно принимает несколько форм: Закон о кибербезопасности (далее — CSL) 2017 г., Закон о защите данных (далее — DSL) 2021 г. и Закон о защите личной информации (далее — PIPL) 202 г.[13] CSL был принят с целью усиления защиты данных, локализации данных и кибербезопасности в интересах национальной безопасности Китая. В этих целях законом регламентирован принцип суверенитета киберпространства, определены обязательства по обеспечению безопасности для поставщиков интернет-продуктов и услуг, подробно описаны обязательства в сфере безопасности для интернет-провайдеров, уточнены правила, касающиеся защиты личной информации, создана система безопасности для объектов КИИ, введены правила транснациональной передачи данных из КИИ. Основываясь на CSL, нормы DSL и PIPL включают новые рекомендации по обороту данных, в том числе персональных, обновленные меры правоприменения и дополнительные ограничения на передачу данных за пределы Китая. Расширяется сфера действия существующих правил оборота данных в Китае, и создается критически новый набор руководящих принципов для компаний, ведущих

[10] URL: https://www.congress.gov/bill/117th-congress/senate-bill/2491/text (дата обращения: 28.04.2022).

[11] URL: https://www.congress.gov/bill/116th-congress/house-bill/6154/ (дата обращения: 28.04.2022).

[12] URL: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa (дата обращения: 28.04.2022).

[13] URL: https://www.wita.org/wp-content/uploads/2021/09/Digital-sovereignty-protectionism-or-autonomy-Hinrich-Foundation-Deborah-Elms-September-2021.pdf (дата обращения: 27.04.2022).

бизнес с китайскими гражданами — причем не только внутри государства, но и за пределами страны согласно экстерриториальному принципу распространения действия нормативного регулирования.

В частности, положения DSL сфокусированы на цели обеспечения правовыми средствами национальной безопасности. Их основу образуют требования к трансграничной передаче данных и к соблюдению правил поставщиками посреднических услуг. Для целей конкретизации правоприменения планируется выпуск специальных каталогов важных данных в различных секторах, подлежащих правовой защите. Более того, статьей 36 DSL установлен запрет для юридических и физических лиц на предоставление доступа к данным иностранным правоохранительным и судебным органам без предварительного одобрения уполномоченных органов Китая. Государством установлен централизованный, унифицированный, эффективный и авторитетный механизм оценки риска безопасности данных, отчетности, обмена информацией, мониторинга и раннего предупреждения. Национальный механизм координации работы по обеспечению безопасности данных должен регламентировать работу соответствующих департаментов для усиления сбора, анализа, исследований и суждений, а также раннего предупреждения об информации о рисках безопасности данных, при этом любые действия по обработке данных, которые влияют или способны повлиять на состояние национальной безопасности, подлежат предварительной проверке на соответствие установленным требованиям.

В ЕС в 2019 г. Европейский парламент принял Закон ЕС о кибербезопасности [13], который установил находящуюся под контролем Агентства ЕС по кибербезопасности (далее — ENISA) систему сертификации для информационных и телекоммуникационных продуктов и услуг компаний, желающих предлагать их на европейском рынке. Так, наряду с конкретными рекомендациями по обеспечению кибербезопасности сетей 5G, он регламентирует строгий контроль доступа, прежде чем той либо иной телекоммуникационной компании дозволяется внести свой вклад в создание и эксплуатацию национальных сетей в контексте ЕС.

Закон ЕС об искусственном интеллекте 2021 г. (далее — Закон об ИИ) представляет собой первую нормативную базу для таких технологий во всем мире, поскольку он вводит систему оценки рисков, предназначенную для регулирования доступа к европейскому рынку на основе оценки категории риска продуктов компании с технологией ИИ. Например, запрещается размещение на рынке, ввод в эксплуатацию или использование систем ИИ государственными органами или от их имени для оценки или классификации благонадежности физических лиц в течение определенного периода времени на основе их социального поведения или известных либо прогнозируемых личностных характеристик. Кроме того, актом внедряется система риск-менеджмента, которая должна полностью контролировать, документировать и оценивать весь жизненный цикл подконтрольной системы ИИ с высоким уровнем риска, предусматривая также регулярное систематическое обновление. Система ИИ с высоким риском должна быть протестирована на соответствие целям ее создания (также должно быть подтверждено, что система не выходит за границы заявленных целей и не совершает действий и не имеет возможностей, которые не являются необходимыми для достижения этих целей) и требованиям законодательства. Тестирование должно быть проведено до вывода системы на рынок или начала ее реального использования. Техническая документация систем ИИ с высоким риском должна быть составлена таким образом, чтобы демонстрировать соответствие системы законодательству и обеспечить надзорным органам получение всей необходимой информации для оценки системы и контроля соблюдения законодательства.

Предусмотрены и иные ограничения при внедрении систем ИИ в пространстве ЕС. Европейские и международные компании приветствовали введение указанной нормативной базы в доселе значительно нерегулируемой области, но выразили обеспокоенность тем, что закон может затормозить инновации, поскольку не известно, насколько строго будут интерпретироваться критерии оценки, и насколько их решения будут совместимы с европейскими стандартами.

Несмотря на то обстоятельство, что Европейской директиве об электронной торговле было более 20 лет, когда были приняты Закон о цифровых услугах (далее — DSA) и Закон о цифровых рынках (далее — DMA), которые решают проблемы, возникшие с появлением новых продуктов и поставщиков услуг на цифровом рынке, она остается краеугольным камнем европейской цифровой стратегии и инструментов цифровой внешней политики, регулирующих доступ к рынкам и институционализирующих европейские нормы. Директива об электронной торговле устанавливает стандарты требований к прозрачности для поставщиков услуг и ответственности по всей бизнес-цепочке, включая поставщиков услуг-посредников, а также общие правила коммерческих коммуникаций. Поскольку цифровая экономика еще больше диверсифицировалась, а личные данные самих частных лиц стали экономическим благом, ЕС обновил свои правила, чтобы обеспечить суверенитет данных своих граждан и компаний.

DSA ввел новые правила в проблемных областях прозрачности с конкретными информационными обязательствами по хранению и коммерциализации пользовательских данных, обработке высказываний ненависти и запретов на участие в обсуждении, а также сообщению о пользователях, которые, как установлено, делятся незаконным контентом. DMA призван создать равные условия для предприятий в эпоху цифровых технологий и обеспечить возможности для инноваций и роста. Он разработан для регулирования деятельности крупных системных

DOI: https://doi.org/10.17816/RJLS106912

онлайн-платформ. Примерами таких «гейткиперов» (хотя до сих пор ни одна компания не была назначена гейткипером) могут быть Amazon, Meta и Alphabet. Малые и средние предприятия, зависящие от них, защищаются требованиями DMA, поскольку гейткиперы больше не могут использовать свои возможности в качестве поставщиков платформ для более заметной рекламы своих товаров и услуг или препятствовать пользователям удалять или отключать определенное программное обеспечение, если они того пожелают. Кроме того, гейткиперы теперь обязаны предоставлять коммерческим пользователям доступ к данным, которые они генерируют при использовании своих платформ, и разрешать третьим сторонам взаимодействовать с их сервисами. Суверенитет данных европейских граждан также защищен недавно принятым Законом ЕС о данных, который разъясняет, при каких условиях частные данные могут быть коммерциализированы.

Закон ЕС о микросхемах 2022 г. призван интегрировать национальные усилия в согласованную европейскую стратегию исследований полупроводников и содействовать коллективным действиям по (повторному) наращиванию производственных мощностей, чтобы обратить вспять тенденцию аутсорсинга производства полупроводников. Чипы (также известные как полупроводники) являются важнейшими компонентами производства цифровых технологий, как в гражданской, так и в военной сферах, и в настоящее время спрос на них настолько высок, что сформирован их глобальный дефицит. В то время как американские компании, такие как Qualcomm, разрабатывают чипы, тем не менее производятся они в основном на Тайване — одна тайваньская компания производит 92 % мировых поставок чипов самого современного типа, создавая крайне уязвимое узкое место в цепочке поставок.

Примечательно, что в Германии цели и политико-стратегический подход федерального правительства к мерам обеспечения безопасности в цифровой сфере, в первую очередь, сфокусирован на охране отношений, возникающих в ходе функционирования объектов КИИ, то есть таких секторов, как энергетика, здравоохранение, информационные технологии и телекоммуникации, транспорт, СМИ и культура, водоснабжение, финансы и страхование, питание, государство и администрация[14], утилизация бытовых отходов[15]. Меры обобщены в Национальной стратегии защиты критически важных инфраструктур (*Nationale Strategie zum Schutz Kritischer Infrastrukturen*) и отраслевом законодательстве. В частности, ключевые вопросы обеспечения безопасности объектов КИИ регламентированы Законом Германии «О Федеральном управлении по информационной безопасности» (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, далее — *BSI-Gesetz*). Так, согласно § 2 *BSI-Gesetz* к информационным технологиям в понимании данного закона относятся все технические средства обработки информации. Информация и системы обработки информации, компоненты и информационные процессы особенно заслуживают защиты, поскольку доступ к ним могут получить только авторизованные лица. Безопасность в информационных технологиях и связанная с этим защита информации и систем обработки информации от атак и несанкционированного доступа по смыслу *BSI-Gesetz* требуют соблюдения определенных стандартов безопасности, чтобы гарантировать основные ценности информационных технологий и цели защиты. При этом состояние безопасности объектов КИИ означает соблюдение определенных стандартов безопасности, влияющих на доступность, целостность или конфиденциальность информации посредством мер безопасности. Правила, регламентированные законом для операторов информационной инфраструктуры, с 2018 г. распространяются и на поставщиков цифровых услуг согласно § 15 *BSI-Gesetz*.

В Австрии цели и политико-стратегические подходы государства к мерам обеспечения безопасности объектов КИИ и кибербезопасности определены, главным образом, Программой обеспечения безопасности критической инфраструктуры 2014 г. (*Österreichisches Programm zum Schutz kritischer Infrastrukturen*, далее — *APCIP*), а также Стратегией кибербезопасности 2021 г. (*Österreichische Strategie für Cybersicherheit*, далее — *ÖSCS*). Ключевыми объектами правовой охраны выступают состояние информационной защищенности, безопасность поставок продуктов питания, транспортных, телекоммуникационных, энергетических и финансовых услуг, а также обеспечение гарантированного предоставления социальных и медицинских услуг[16]. В частности, конкретные меры в рамках текущей работы по корректировке уголовного законодательства с учетом положений *APCIP* и *ÖSCS* должны предусматривать квалификационные положения о предупреждении нарушений в деятельности предприятий и организаций, составляющих объекты КИИ, а также изменения, направленные на совершенствование правовых норм, охраняющих от посягательств информационные системы.

Изложенная европейская цифровая внешняя политика уже значительно продвинула суверенитет данных европейских граждан и выровняла игровое поле цифрового рынка, одновременно усилив защиту от угроз кибербезопасности, что внесло значительный вклад в обеспечение европейского цифрового суверенитета. Однако специалисты отмечают, что ЕС не сможет достичь цифрового суверенитета в одиночку — на данный момент не хватает производственных мощностей, крупных компаний,

[14] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung).

[15] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0).

[16] См.: Masterplan APCIP zur Gewährleistung der Versorgungsicherheit bei Lebensmitteln, Verkehrs-, Telekommunikation-, Energie- und Finanzdienstleistungen wie auch auf eine gesicherte Versorgung mit Sozial- und Gesundheitsdienstleistungen.

DOI: https://doi.org/10.17816/RJLS106912

занимающихся цифровыми технологиями, и, в некоторой степени, также соответствующей цифровой инфраструктуры. Поэтому трансатлантическое сотрудничество и действия необходимы для обеспечения цифрового суверенитета и геополитического положения ЕС, для дальнейшего обеспечения справедливой рыночной конкуренции и защиты гражданских свобод граждан. Этот же тезис применим и к США. Например, на долю США и ЕС приходится 21 % мировых мощностей по производству полупроводников, но при этом 43 % мирового потребления цифровых устройств, что свидетельствует о потенциально опасной зависимости от китайских производителей [14].

3. Уголовно-правовые механизмы защиты цифрового суверенитета

Важно отметить, что за рубежом правовые механизмы обеспечения цифрового суверенитета предусмотрены не только в контексте стратегического планирования развития государства и общества или установления регуляторных требований, но также и в уголовно-правовой сфере. В данном разделе с учетом ограниченного объема исследования представлены отдельные доступные примеры механизмов уголовно-правовой защиты суверенитета анализируемых юрисдикций в цифровом пространстве.

В США нарушение обязанностей в рамках BSA биржами и администраторами криптовалют влечет уголовную ответственность. Так, непредставление отчета об операциях (31 U.S. Code § 5315), а также структурирование финансовых сделок в целях неисполнения обязанности предоставления такой отчетности (31 U.S. Code § 5324) наказываются тюремным заключением на срок до пяти лет и (или) штрафом в 250 000 долларов США (18 U.S. Code § 3571), если преступление совершено без отягчающих обстоятельств. Наличие последних (например, нарушение нескольких законов США одновременно либо превышение порогового значения количества вовлеченных в незаконные операции денежных средств, которое составляет 100 000 долларов США за последние 12 месяцев) предполагает назначение более строгого наказания за содеянное: десять лет тюремного заключения и (или) штраф в двойном размере в соответствии с подсекциями (b)3 и (c)3 секции 3571 титула 18 Свода законов США (т.е. 500 000 долларов США для физических лиц и 1 000 000 долларов США для организаций). Аналогичным образом наказываются и другие деяния, связанные с деятельностью по фиксации и предоставлению отчетности по транзакциям валютных инструментов (31 U.S. Code § 5322)[17]. Кроме того, действия на фондовых или товарных рынках, которые направлены на побуждение к принятию участниками тех либо иных инвестиционных решений на основе ложных данных, является мошенничеством. Оно может быть выражено в прямом хищении инвестиционных средств, в том числе биржевыми брокерами, манипулировании на рынке акций, искажении финансовой отчетности публичной компании и др.

Поскольку в законодательстве США предусмотрена категория криптобумаг, о которой было сказано выше, постольку Комиссия по ценным бумагам и биржам США (далее — SEC) относит к мошенническим действия на рынке ценных бумаг, совершенные с помощью цифровых финансовых инструментов, которые искусственно отождествляются с денежными средствами. Этот вывод следует из анализа решения, принятого судом по делу Трендона Т. Шейверс, обвиненного в создании *Bitcoin* пирамиды[18]. Коллективный ущерб инвесторов составил 265 678 *Bitocin*, или более 149 миллионов долларов США[19]. В судебном решении было определено, что использованная в преступной деятельности криптовалюта есть ни что иное как деньги, а следовательно, инвестиции участников были ценными бумагами. Несмотря на некоторое ограничение использования криптовалюты, она, тем не менее, может быть обменена на фиатные валюты. С этих позиций судья решил, что *Bitcoin* представляет собой валюту или особую форму денег, а лица, желающие инвестировать в «проект» Шейверса, осуществляют инвестиционную деятельность в денежной форме. Совершение таких противоправных действий является преступным по смыслу секции 24 закона США о ценных бумагах (Securities Act of 1933) и наказывается штрафом и (или) тюремным заключением на срок до пяти лет[20].

В Китае в дополнение к трем краеугольным актам общего правового режима защиты данных и кибербезопасности (CSL, DSL и PIPL) в отдельных законах и нормативных актах регламентированы положения о конфиденциальности и защите данных, в том числе в уголовно-правовой сфере. Например, в соответствии со статьей 63 CSL виновные в совершении преступлений в сфере кибербезопасности лица пожизненно лишаются права заниматься управлением кибербезопасностью и ключевыми сетевыми операциями. При этом совершение уголовно наказуемого деяния в цифровом пространстве подлежит уголовному преследованию в соответствии с законом (статья 74 CSL). Аналогичные правовые механизмы регламентированы статьями 50-52 DSL. Тем самым, сложившееся в Китае на законодательном уровне регулирование, направленное на обеспечение цифрового суверенитета государства, с позиции структуры уголовного законодательства является так называемым дополнительным уголовным правом, раскрывающим специальные признаки и меры ответственности

[17] URL: https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (дата обращения: 28.04.2022).

[18] URL: https://www.sec.gov/news/press-release/2013-132#.VHIOy4uJndm (дата обращения: 28.04.2022).

[19] Sec. & Exch. Comm'n v. Shavers. No. 4:13-CV-416, 2014 WL 4652121. at *1 (E.D. Tex. Sept. 18, 2014). URL: https://www.law.du.edu/documents/corporate-governance/securities-matters/shavers/SEC-v-Shavers-No-4-13-CV-416-E-D-Tex-Sept-18-2014.pdf (дата обращения: 28.04.2022).

[20] URL: https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf (дата обращения: 28.04.2022).

в случае, когда деяние посягает на отношения в сфере обеспечения цифрового суверенитета.

В Германии и Австрии защита суверенитета государства в киберпространстве уголовно-правовыми средствами реализуется, прежде всего, в контексте противодействия легализации (отмыванию) преступных доходов при помощи цифровых валют, посягательствам на объекты КИИ, а также совершению киберпреступлений.

Так, 11 февраля 2021 г. Бундестаг Германии принял закон о совершенствовании борьбы с отмыванием денег уголовно-правовыми средствами с учетом положений Директивы ЕС 2018/1673 о борьбе с отмыванием денег. Теперь не имеет значения, какие именно преступления или проступки предшествовали действию, связанному с легализацией доходов. Необходимо доказать лишь факт, что такое лицо знало о преступном характере происхождения какого-либо экономического блага. Таким образом, все преступления и проступки предзнаменуют легализацию доходов, в том числе с помощью цифровых валют. При этом понятие предмета преступления было расширено и в настоящий момент включает активы всех видов, независимо от того, являются ли они физическими или бестелесными, движимыми или недвижимыми, материальными или нематериальными. Более того, юридические титулы или документы в любой форме (в том числе в электронном или цифровом виде), подтверждающие право собственности или права на такие активы и ценности, также согласно внесенным изменениям отнесены к предмету анализируемого преступления[21].

В Австрии аналогичные по своему содержанию изменения были непосредственно внесены в конструкцию состава преступления легализации (отмывания) преступных доходов. В § 165 *ÖStGB* прямо закреплено, что нет необходимости ни в том, чтобы преступник был осужден за предикатное преступление, ни в том, чтобы были установлены все фактические элементы или все обстоятельства, связанные с предшествующей преступлению деятельностью, включая и личность преступника. Под активами по смыслу данной нормы австрийского уголовного закона понимаются активы всех видов, в том числе юридические документы или акты в цифровой форме, которые доказывают право собственности или права на активы, единицы виртуальных валют, увеличение стоимости, связанное с этими правами или правами, основанными на них, и, более того, цифровой актив, полученный в результате преобразования преступного дохода.

Нарушение требований *BSI-Gesetz*, несанкционированный доступ к информации и иные преступные посягательства на объекты КИИ подлежат уголовному преследованию в контексте противодействия киберпреступлениям. К последним в Германии относятся все преступления, направленные против сети Интернет, дополнительных сетей данных информационных систем или их данных, а также объектов КИИ. В этом отношении *StGB* содержит самостоятельный состав преступления, предусмотренный § 303a, который устанавливает ответственность за неправомерное удаление, преобразование, приведение в непригодное состояние и изменение данных. Распространение вредоносного программного обеспечения, направленного на уничтожение данных и (или) блокирование/саботирование бизнес-процессов, является актом киберсаботажа, что подпадает под действие § 303b *StGB*. При этом особо серьезные случаи киберсаботажа наказываются лишением свободы на срок от шести месяцев до десяти лет. К таким случаям относится, например, нанесение ущерба снабжению населения товарами или услугами первой необходимости либо национальной безопасности Германии. Поскольку объекты КИИ представляют исключительную важность в процессе обеспечения существования государства и общества, постольку любое несанкционированное воздействие на них с целью нарушения их функционирования либо извлечения иной выгоды будет преследоваться в уголовном порядке в соответствии с положениями раздела XXVII *StGB* о киберпреступлениях. При этом посягательство на какой-либо конкретный объект КИИ, которое привело к тяжким последствиям, может быть квалифицировано по совокупности преступлений, регламентированных §§ 303a, 303b и другими нормами *StGB*, например, о шпионаже данных (§ 202a), перехвате данных (§ 202b), вмешательстве в железнодорожное, морское и воздушное движение (§ 315), нарушении работы телекоммуникационных систем (§ 317), повреждении важных объектов (§ 318) и др.

Как и в Германии, в Австрии преступные посягательства на компьютерные системы или объекты КИИ могут быть осуществлены посредством совершения различных действий. Например, в результате незаконного доступа к компьютерной системе (§ 118a *ÖStGB*), нарушения тайны телекоммуникаций (§ 119 *ÖStGB*), неправомерного перехвата данных (§ 119a *ÖStGB*), причинения серьезного материального ущерба объекту КИИ (§ 126 *ÖStGB*), повреждения данных и существенных компонентов объекта КИИ (§ 126a *ÖStGB*), нарушения функциональности компьютерной системы либо являющейся неотъемлемой частью объекта КИИ компьютерной системы (§ 126b *ÖStGB*), ввоза, создания, хранения, изменения компьютерных программ для целей использования при совершении перечисленных преступлений, за исключением причинения серьезного материального ущерба объекту КИИ (§ 126c *ÖStGB*) и др. При этом в уголовном законодательстве Австрии прямо закреплены понятия компьютерной системы и КИИ в соответствии с § 74 *ÖStGB*. Первая понимается как совокупность отдельных или подключенных друг к другу устройств, используемых для автоматизированной обработки данных. Вторая — как объекты, установки, системы или их части, которые имеют существенное значение для поддержания общественной безопасности,

[21] Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche vom 9. März 2021 // Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 10. Ausgegeben zu Bonn am 17. März 2021. P. 327.

национальной обороны или защиты гражданского населения от опасностей войны, функционирования общественной информации и коммуникационных технологий, предотвращения или борьбы со стихийными бедствиями, служба общественного здравоохранения, общественное снабжение водой, энергией и товарами первой необходимости, общественная утилизация отходов и канализация, общественный транспорт. Несмотря на то обстоятельство, что не все диспозиции норм *ÖStGB* отсылают к указанным понятиям компьютерной системы или КИИ, тем не менее, представляется допустимым утверждение о возможности квалификации конкретного деяния по совокупности преступлений, признаки которых определены не только перечисленными, но и другими составами преступлений, как, например, преднамеренная экологически опасная эксплуатация систем (§ 181d *ÖStGB*).

Таким образом, представленный анализ правовых механизмов защиты цифрового суверенитета в сравнительно-правовом аспекте позволяет сделать обоснованный вывод в пользу тезиса, что именно цифровые технологии сегодня становятся основой поддержки конкурентоспособности не только бизнес-сообщества, но, прежде всего, государства. Проблема состоит в том, что в основу цифровизации общественных отношений, охватываемых *jus publicum*, и государственности сегодня положены решения и алгоритмы, которые не только разработаны и внедрены в практику частными компаниями (преимущественно зарубежными), но, прежде всего, предполагают построение сервис-ориентированной архитектуры отношений, исключающей самостоятельность (цельность, завершенность) любого цифрового продукта (товара, услуги). В таких условиях значительно возрастают риски утраты независимости и верховенства власти государства, если отсутствуют какие-либо альтернативы.

Зарубежный опыт свидетельствует о тщательной проработке правовых механизмов обеспечения цифрового суверенитета. Такие механизмы находят свое непосредственное отражение не только в положениях отраслевого, в том числе и уголовного, законодательства, но, прежде всего, документах стратегического планирования. Однако необходимо обратить внимание на то обстоятельство, что большинство законодательных инициатив в области защиты цифрового суверенитета все еще сфокусировано не на внутреннем (цифровом) пространстве, а на внешнем, т.е. касается лишь внешних форм выражения исследуемых отношений в объективированном мире. Тем самым, цифровое пространство пока так и оставлено без «инфраструктуры», которая может обеспечить превентивную функцию защиты национального суверенитета в новых условиях. Представляется важной в связи с этим разработка не только ординарных (внешних), но также экстраординарных (внутренних) механизмов правового обеспечения цифрового суверенитета государства по наиболее ключевым направлениям.

СПИСОК ЛИТЕРАТУРЫ

1. Тенденции цифровизации исполнительной власти в зарубежных странах: научно-практическое пособие / Т.И. Чурсина, Н.Б. Крысенкова, Ф.А. Лещенков, Н.Ю. Трещетенкова; отв. ред. А.Н. Пилипенко; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. М.: Инфотропик Медиа, 2021. 232 с.

2. Хилюта В.В. Дематериализация предмета хищения и вопросы квалификации посягательств на виртуальное имущество // Журнал российского права. 2021. № 5. С. 68–82.

3. Саркисян Т. Интеграционный «план ГОЭЛРО» для XXI века // Россия в глобальной политике. 2021. № 3. С. 136–149.

4. Формирование национального цифрового суверенитета в условиях дифференциации пространственного развития / Л.С. Леонтьева, М.В. Кудина, А.С. Воронов, С.С. Сергеев // Государственное управление. Электронный вестник. Февраль, 2021. Выпуск № 84. С. 277–299.

5. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) / В.А. Никонов, А.С. Воронов, В.А. Сажина и др. // Вестник Томского государственного университета Философия. Социология. Политология. 2021. № 60. С. 206–216.

6. Мартиросян А. Реалии цифрового суверенитета в современном мире // Международная информационная безопасность. 2021. № 3. С. 28–35.

7. Право техногенной цивилизации: современные трансформации и векторы развития: материалы Международной студенческой научно-практической конференции (Москва, 24 октября 2019 г.) / Ю.Н. Кашеварова, И.А. Шулятьев, Э.К. Сайфуллин. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2021. 222 с.

8. Концепция цифрового государства и цифровой правовой среды: монография / Н.Н. Черногор, Д.А. Пашенцев, М.В. Залоило и др.; под общ. ред. Н.Н. Черногора, Д.А. Пашенцева. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации: Норма: ИНФРА-М, 2021. 244 с.

9. Замышляев Д.В., Печников Н.А. Международно-правовое регулирование системы противодействия отмыванию доходов, полученных преступным путем, и финансированию терроризма // Международное публичное и частное право. 2016. № 6. С. 25–29.

10. Boberach M., Neuburger R. Zukunftspfade Digitales Deutschland 2020 // HMD. 2014. Vol. 51. P. 762–772.

11. Гаврилов Е.О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты // Вестник КемГУ. Гуманитарные и общественные науки. 2020. № 4 (2). С. 146–152.
12. Meltzer P.E. Keeping Drug Money from Reaching the Wash Cycle: A Guide to the Bank Secrecy Act // Banking Law Journal. 1991. № 108 (3). P. 230–255.
13. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н.А. Голованова, А.А. Гравина, О.А. Зайцев и др. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации; ООО «ЮРИДИЧЕСКАЯ ФИРМА КОНТРАКТ», 2019. 212 с.
14. Bendiek A., Stürzer I. Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council // SWP Comment. 2022/C20. DOI: 10.18449/2022C20.

REFERENCES

1. Chursina TI, Krysenkova NB, Leschenkov FA et al. Trends of digitalization of executive power in foreign countries: a scientific and practical guide. Ed. by AN Pilipenko; Institute of Legislation and Comparative Jurisprudence under the Government of the Russian Federation. Moscow: Infotropik Media, 2021. 232 p. (In Russ.).
2. Khilyuta VV. Dematerialization of the object of theft and issues of qualification of encroachments on virtual property. *Journal of Russian Law*. 2021;(5):68–82. (In Russ.).
3. Sarkisyan T. The integration "GOELRO plan" for the XXI century. *Russia in Global politics*. 2021;(3):136–149. (In Russ.).
4. Leontieva LS, Kudina MV, Voronov AS et al. Formation of national digital sovereignty in the conditions of differentiation of spatial development. *Public administration. Electronic bulletin.* February, 2021;(84):277–299. (In Russ.).
5. Nikonov VA, Voronov AS, Sazhina VA et al. Digital sovereignty of the modern state: content and structural components (based on the materials of expert research). *Bulletin of Tomsk State University Philosophy. Sociology. Political science.* 2021;(60):206–216. (In Russ.).
6. Martirosyan A. Realities of digital sovereignty in the modern world. *International information security*. 2021;(3):28–35. (In Russ.).
7. Kashevarova YuN, Shulyatyev IA, Saifullin EK. The law of technogenic civilization: modern transformations and vectors of development: materials of the International Student Scientific and Practical Conference (Moscow, October 24, 2019). Moscow: Institute of Legislation and Comparative Jurisprudence under the Government of the Russian Federation, 2021. 222 p. (In Russ.).
8. Chernogor NN, Pashentsev DA, Zaloilo MV. The concept of the digital state and the digital legal environment: monograph. Ed. by Chernogor NN, Pashentsev DA. Moscow: Institute of Legislation and Comparative Law under the Government of the Russian Federation: Norm: INFRA-M, 2021. 244 p. (In Russ.).
9. Zamyshlyaev DV, Pechnikov NA. International legal regulation of the system of countering the laundering of proceeds from crime and the financing of terrorism. *International public and private law*. 2016;(6):25–29. (In Russ.).
10. Boberakh M, Neuburger R. Zukunftspfade Digitales Deutschland 2020. *HMD*. 2014;(51):762–772.
11. Gavrilov EO. Digital sovereignty in the context of globalization: philosophical and legal aspects. *Bulletin of KemGU. Humanities and social sciences*. 2020;4(2):146–152. (In Russ.).
12. Meltzer PE. Preventing drugs from entering the Laundering Cycle: A Guide to the Law on Bank Secrecy. *Journal of Banking Law*. 1991;108(3):230–255.
13. Golovanova NA, Gravina AA, Zaitsev OA et al. Criminal-jurisdictional activity in the conditions of digitalization: monograph. Moscow: Institute of Legislation and Comparative Law under the Government of the Russian Federation; LLC "LAW FIRM CONTRACT", 2019. 212 p. (In Russ.).
14. 14. Bendik A, Shturzer I. Promoting Europe's Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council. *SWP Comment. 2022/C20*. DOI: 10.18449/2022C20.

ОБ АВТОРЕ

Денис Андреевич Печегин, кандидат юридических наук, старший научный сотрудник; e-mail: crim5@izak.ru; ORCID: https://orcid.org/0000-0001-6499-9966

AUTHOR INFORMATION

Denis A. Pechegin, phd, senior researcher; e-mail: crim5@izak.ru; ORCID: https://orcid.org/0000-0001-6499-9966