Научная статья
УДК 34.096
doi: 10.17223/15617793/518/24

Регулирование криптографической деятельности в России: проблемы и перспективы развития

Алексей Владимирович Минбалеев[1], Кирилл Сергеевич Евсиков[2, 3]

[1, 3]Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), Москва, Россия
[2] Тульский государственный университет, Тула, Россия
[1] avminbaleev@msal.ru
[2, 3] aid-ltd@yandex.ru

Аннотация. Исследование направлено на развитие предложений по развитию регулирования криптографической деятельности в России. Выявлены пробелы правового регулирования в данной сфере. Доказывается необходимость разработки и принятия специального закона, посвящённого криптографической деятельности, что будет способствовать развитию использования современных технологий защиты информации, в том числе квантовых коммуникаций. Представлена структура данного акта, а также цели, которые должны быть достигнуты им.
Ключевые слова: законодательство о криптографии, законопроект о криптографической деятельности, защита информации, информационная безопасность, информационное право, квантовые коммуникации, криптографическая деятельность, правовое обеспечение информационной безопасности, правовое регулирование, развитие законодательства

***Источник финансирования*:** исследование выполнено за счет гранта Российского научного фонда № 24-18-00950, https://rscf.ru/project/24-18-00950/.

***Для цитирования*:** Минбалеев А.В., Евсиков К.С. Регулирование криптографической деятельности в России: проблемы и перспективы развития // Вестник Томского государственного университета. 2025. № 518. С. 211–219. doi: 10.17223/15617793/518/24

Original article
doi: 10.17223/15617793/518/24

Regulation of cryptographic activities in Russia: Problems and prospects of development

Aleksey V. Minbaleev[1], Kirill S. Evsikov[2, 3]

[1, 3] Kutafin Moscow State Law University, Moscow, Russian Federation
[2] Tula State University, Tula, Russian Federation
[1] avminbaleev@msal.ru
[2, 3] aid-ltd@yandex.ru

Abstract. The aim of the article is to formulate proposals for enhancing the effectiveness of the legal regulation of cryptographic activities in the Russian Federation. The research material consists of the norms of Russian legislation governing cryptographic activities, the emerging law enforcement practice in this field, and doctrinal studies. The research methods employed include the method of systems analysis, which was used to examine the current state and specific features of regulating cryptographic activities in the Russian Federation, and the method of legal modeling, which was used to develop models for improving cryptography legislation. The study identified the range of public relations regulated by legislation on cryptographic activities, which include: relations concerning the creation of cryptographic information protection tools, including the regulation of the certification process; relations concerning the use of such tools, as well as their circulation, including the export and import of equipment; relations concerning the provision of services related to cryptographic activities; relations concerning the control of cryptographic activities, as well as other administrative relations. It was established that this list of relations may develop further. An analysis of the experience in applying legislation in the field of cryptographic activities revealed a number of gaps in the legal regulation of this sphere. In this regard, models for improving the regulation of cryptographic activities were developed: 1) a model associated with introducing amendments to existing legislation; 2) a model implemented by adding a corresponding section to an Information Code; 3) a model associated with creating a separate federal law. A number of risks and implementation difficulties were identified regarding the first two models. An analysis of the emerging relations in the field of cryptographic activities, as well as the current legislation in this field, led to the conclusion that a special federal law dedicated to cryptographic activities is objectively necessary today. Its adoption could significantly contribute to the development and use of modern information protection technologies, including quantum communications. The article presents the structure of this proposed act, as well as the goals it should achieve. It is substantiated

that in the development of a draft federal law on cryptographic activities, it is of paramount importance that this work contributes to the formation of an effective domestic competitive cryptographic system.
Keywords: legislation on cryptography, draft law on cryptographic activities, information protection, information security, information law, quantum communications, cryptographic activities, legal provision of information security, legal regulation, development of legislation

***Financial support*:** The research was supported by the Russian Science Foundation, Project. No. 24-18-00950, https://rscf.ru/project/24-18-00950

***For citation*:** Minbaleev, A.V. & Evsikov, K.S. (2025) Regulation of cryptographic activity in Russia: problems and prospects of development. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 518. pp. 211–219. (In Russian). doi: 10.17223/15617793/518/24

Введение

Средства криптографической защиты информации (далее – СКЗИ) стали неотъемлемой частью информационного общества, цифрового государства и экономики данных. Под криптографией (шифрованием) понимаются действия по конвертации информации в форму, которая не читаема для третьих лиц. Прочесть зашифрованные данные может только лицо, имеющее секретный ключ, а, значит, даже в случае перехвата конфиденциальной информации, она будет недоступна злоумышленнику.

Российская криптографическая школа является одной из сильнейших, что обеспечивается наличием собственных алгоритмов шифрования; сформированной в советский период высококлассной научной школой; развитой экосистемой, включающей исследовательские организации, производителей оборудования и исполнителей услуг в сфере криптографии; жестким контролем со стороны государства, который гарантирует качество отечественного оборудования через систему сертификации, а также качество оказания услуг в сфере криптографии, через систему лицензирования.

Все это обеспечивается совокупностью несистематизированных и разрозненных норм, рассредоточенных в нормативных правовых актах разного уровня. Именно их мы и предлагаем называть законодательством о криптографии. Это не устоявшийся термин и нам известно лишь о единичных случаях его использования в научных публикациях [1] и нормативно-технических актах (см., например ГОСТ Р ИСО/МЭК 27002-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности, утвержден и введен в действие Приказом Росстандарта от 20.05.2021 № 416-ст). При этом иной концепт, объединяющий указанные правила поведения, в отечественном праве отсутствует. Также можно говорить о правовом институте правового регулирования отношений в сфере криптографии, активно формируемом сегодня в рамках подотрасли информационного права – правового регулирования информационной безопасности.

Такой научный вакуум объясняется отсутствием должного внимания у юридической науки к исследованиям данных правоотношений. Хотя вопросам информационной безопасности отечественные правоведы посвящают множество работ [2–5], но сферу криптографии, являющуюся ядром данных общественных отношений, они, к сожалению, не изучают. Во многом это детерминировано тем, что значительная часть отношений в сфере криптографии не может быть рассмотрена в публичной плоскости, так как относится к информации ограниченного доступа. Понимая данный факт, многие просто избегают даже упоминания правоотношений в сфере криптографии в рамках системы правового обеспечения информационной безопасности.

Возможность проведения открытых правовых исследований правоотношений в сфере криптографии подтверждается анализом схожих по уровню конфиденциальности общественных отношений, например, в сфере оперативно-розыскной деятельности, в отношении которой сегодня имеется и открытая специальная учебная литература [6].

Результатом этого подхода является ситуация, когда криптография стала terra incognita для юридического сообщества, которое не только не создало для регламентации этой деятельности специальный нормативный правовой акт, но и не включило в законодательство Российской Федерации даже определение термину криптография. В связи с этим можно констатировать, что сегодня отечественная криптография развивается в рамках разрозненных ведомственных актов, которые дают возможность контролировать стабильный рынок СКЗИ, но, к сожалению, не дают возможности стимулировать его инновационное развитие. Этот вывод сделан в том числе на основе ряда исследований правового регулирования отношений в сфере квантовых коммуникаций в Российской Федерации [7–9].

В связи с этим в данной статье поставлена *цель* – сформировать конкретные предложения по повышению эффективности правового регулирования криптографической деятельности в Российской Федерации. Для этого авторы:

– проанализировали существующие складывающиеся правоотношения в сфере криптографической деятельности;

– выявили основные нормы отечественного права, регламентирующие криптографическую деятельность, и систематизировали их;

– определили место и границы правоотношений в сфере криптографической деятельности;

– обосновали необходимость разработки и принятия, а также предложили структуру специального федерального закона о криптографической деятельности в Российской Федерации.

Регулирование криптографической деятельности в Российской Федерации

Анализ отечественного законодательства в сфере информационной безопасности свидетельствует о том, что в России, к сожалению, отсутствует системный подход к регулированию криптографической деятельности, что привело к существованию значительного количества правовых пробелов и коллизий, а также к сохранению в действии морально устаревших нормативных правовых актов. Среди них можно выделить следующие.

1. В Российской Федерации действует ряд несогласованных нормативных правовых актов разного уровня, регулирующих криптографическую деятельность. Иногда противоречия носят концептуальный характер, что не препятствует их одновременному применению. Не вызывает сомнений, что такой подход не только создает путаницу в правоприменении, но и способствует снижению общей и специальной правовой культуры в процессе осуществления криптографической деятельности, что сказывается на уровне информационной безопасности российских предприятий и органов власти. Например, в ч. 1 ст. 5 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» определено, что существуют только три вида такой подписи: простая электронная подпись и усиленная неквалифицированная электронная подпись, усиленная квалифицированная электронная подпись. При этом федеральные органы власти, издавая официальные документы в сфере шифрования, используют термин цифровая подпись (Стандарт Банка России «Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect. Требования» СТО БР ФАПИ.СЕК-1.6-2024. Принят и введен в действие приказом Банка России от 07.10.2024 № ОД-1615) или электронная цифровая подпись (далее – ЭЦП) (см.: Приказ СФР от 06.07.2023 № 1319 «О защищенном обмене документами в электронном виде с применением электронной цифровой подписи для целей обязательного социального страхования»). Данный термин был закреплен в ФЗ от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», который утратил свою силу.

В случае использования термина ЭЦП органы власти подразумевают усиленную квалифицированную электронную подпись, но ни в одном акте о наличии подобной эквивалентности не оговаривается. В связи с этим вызывает озабоченность, что использование неточных терминов допускается даже в актах Правительства Российской Федерации, где встречается термин ЭЦП (например, в Постановлении Правительства РФ от 13.09.2021 № 1547). Подобная терминологическая рассогласованность в законодательстве о криптографии во многом обусловлена активным использованием термина ЭЦП в нормативно-технических документах, например, в ГОСТ 34.10-2018. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи (введен в действие приказом Росстандарта от 04.12.2018 № 1059-ст). Очень часто в сфере информационной безопасности нормативные правовые акты формируется на основе нормативно-технического регулирования и имплементация норм из них происходит без учета действующих вышестоящих по юридической силе правовых норм, что вызывает сложности в последующем правоприменении.

2. В Российской Федерации действуют устаревшие акты, регулирующие криптографическую деятельность. К ним относится приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», который действует более 20 лет без внесения в него изменений и дополнений, что является уникальным случаем для отечественного законодательства об информационной безопасности. Причиной правовой стабильности стала ликвидация Указом Президента РФ от 11.03.2003 № 308 «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации» ФАПСИ. Как следствие, документ оперирует отсылками к отмененным законам и подзаконным нормативным правовым актам, говорит об СКЗИ «сертифицированном ФАПСИ» и об организациях, «лицензированных ФАПСИ». При этом сама инструкция содержит правила, утратившие актуальность в связи с развитием информационных технологий, например, при использовании технологий квантового распределения ключа соблюсти все алгоритмы, закрепленные в документе, не представляется возможным [10].

Указ Президента Российской Федерации от 03.04.1995 № 334 также запрещает органам публичной власти использовать ЭЦП и СКЗИ без сертификата ФАПСИ. Этим же документом запрещен ввоз на территорию Российской Федерации шифровальных средств иностранного производства без лицензии Министерства внешних экономических связей Российской Федерации, которое упразднено в 1998 году. Все это позволяет говорить о необходимости значительной ревизии и систематизации законодательства о криптографической деятельности в России.

3. В законодательстве о криптографии границы полномочий органов публичной власти не всегда четко распределены. Например, Положение о сертификации средств защиты информации, утвержденное Постановлением Правительства РФ от 26.06.1995 № 608, в котором определено, что действуют три системы сертификации, которые должны работать по собственному положению: при Федеральной службе по техническому и экспортному контролю (ФСТЭК России); при Федеральной службе безопасности Российской Федерации (ФСБ России); при Министерстве обороны Российской Федерации. Все три системы успешно функционируют, но положения утверждены только Приказом ФСТЭК России (приказ от 03.04.2018 № 55 (ред. от 19.09.2022) «Об утверждении Положения о системе сертификации средств защиты информации» и Приказом Министра обороны Российской Федерации (приказ от 29.09.2020 № 488).

ФСБ России утвердило Положение, регламентирующее не порядок сертификации, а порядок разработки, производства, реализации и эксплуатации СКЗИ (Приказ ФСБ РФ от 09.02.2005 № 66, далее – ПКЗ-2005). При этом на оборудование, созданное в рамках данного документа, орган публичной власти сертификат выдает. ПКЗ-2005 является одним из ключевых документов, являющихся основой отечественного законодательства о криптографии. Именно в нем определено оборудование, которое подпадает под термин СКЗИ: средства шифрования; средства имитозащиты; средства электронной цифровой подписи; средства кодирования; средства изготовления ключевых документов; ключевые документы.

Перечень содержит термин ЭЦП, что создает правовой пробел, так как, согласно буквальному толкованию норм данного акта, ФСБ России не должно регулировать отношения в сфере создания усиленной квалифицированной электронной подписи, хотя фактически это происходит. Есть и иные сложности, возникающие в процессе применения данного акта. В первую очередь они касаются распределения полномочий по сертификации средств защиты информации. Фактически ФСБ России, приняв данный документ, определило свою компетенцию в сфере сертификации средств защиты данных. Это означает, что полномочия по сертификации всех остальных средств защиты данных разделили Министерство обороны Российской Федерации, осуществляющее данную деятельность для собственных нужд, и ФСТЭК России, осуществляющее данную деятельность во всех остальных случаях. Таким образом, ФСТЭК России сертифицирует технологии, называемые средства защиты информации (далее – СЗИ), а ФСБ России – СКЗИ. Однако проблема возникает тогда, когда частью СЗИ является система шифрования, что в современных условиях цифровизации встречается повсеместно. В Положении Министерства обороны Российской Федерации такой случай предусмотрен и ведомство требует, чтобы производитель прикладывал сведения о наличии сертификата соответствия ФСБ России. В Положении ФСТЭК России, к сожалению, этот случай не предусмотрен.

Не вызывает сомнений, что СЗИ является более объемной категорией и должна включать СКЗИ, в то же время само СКЗИ уже не может существовать отдельно, а дополняется иными технологиями защиты данных. В этой ситуации у производителя нет иного выхода, чем проходить двойную сертификацию, что нарушает Положение о сертификации 1995 г., так как компетенции органов публичной власти фактически накладываются. Это лишь один из примеров, когда законодательство о криптографии не смогло осуществить четкое разграничение компетенций органов публичной власти.

Важно отметить, что подобная ситуация не является уникальной, например, в США регулированием криптографии занимаются три организации: Федеральная комиссия по связи (FCC) регулирует криптографию в системах беспроводной связи; Агентство национальной безопасности разрабатывает безопасные криптографические системы для государственных учреждений; Агентство по кибербезопасности и безопасности инфраструктуры (CISA) предоставляет рекомендации по лучшим практикам криптографии. И на практике также часто возникают проблемы, аналогичные российским.

4. В законодательстве о криптографии существует и ряд правовых пробелов. Например, отсутствие регулирования ряда вопросов использования СКЗИ иностранного производства. Данное оборудование является ограниченным к ввозу на территорию ЕАЭС (см. раздел 2.19 «Шифровальные (криптографические) средства» приложения № 2 к Решению Коллегии Евразийской экономической комиссии от 21 апреля 2015 г. № 30 «О мерах нетарифного регулирования»), однако сам импорт шифраторов не запрещен и в некоторых случаях даже упрощен (см.: Постановление Правительства РФ от 09.05.2022 № 834 «Об установлении особенностей ввоза в Российскую Федерацию шифровальных (криптографических) средств и товаров, их содержащих»). На это оборудование не распространяет свое действие ПКЗ-2005 (пункт 5), а значит, сертификат ФСБ России импортер получить не может. Кроме того, пункт 1 Положения о сертификации средств защиты информации закрепил, что криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России. Таким образом, и оборот, и использование импортных СКЗИ не запрещены, и не разрешены, что вызывает вопросы на практике. Например, в сетях банкоматов длительное время использовалась Triple DES, система SWIFT, которая основана на оригинальной иностранной криптосхеме.

Более того, в отечественном законодательстве о криптографии нет норм, определяющих порядок оценки СКЗИ в качестве «отечественного оборудования». То есть ничто не запрещает в импортируемое оборудование вставить корпус отечественного производства и указывать в качестве места его происхождения территорию Российской Федерации.

Все это также обусловливает необходимость совершенствования системы регулирования законодательства о криптографии.

Модели совершенствования законодательства о криптографии

Исходя из того, что криптография связана с вопросами защиты информации, то криптографическую деятельность необходимо рассматривать в качестве предмета информационного права, в частности правового регулирования информационной безопасности.

При этом в Федеральном законе «Об информации, информационных технологиях и о защите информации» о криптографической деятельности упоминается только в одной норме, регламентирующей взаимодействие в электронной форме органов публичной власти с организациями и юридическими лицами. В ней закреплено, что государство должно обеспечить при обмене электронными документами соблюдение правил и

принципов, установленных национальными стандартами Российской Федерации в области криптографической защиты информации (ч. 2.3 ст. 13 Федерального закона от 27.07.2006 № 149-ФЗ). Этого явно не достаточно для регламентации криптографической деятельности, учитывая ее значение для общества и государства в условиях активного развития сферы информационной безопасности, в том числе новых направлений, связанных с использованием технологий квантовых коммуникаций. Следует отметить, что подобный «юридический минимализм» законодатель проявил и в вопросе регулирования защиты информации, которому в законе посвящена статья 16, включающая 6 частей. В ней определены виды деятельности, относимые законом к защите информации; обязанности обладателя информации и оператора информационной системы в сфере защиты информации; особенности регулирования защиты информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов и т.д. Представляется логичным для совершенствования законодательства о криптографии внести изменения в данную статью или добавить новую статью в федеральный закон. Однако, как показывает анализ изменений и дополнений в этот нормативный правовой акт, подобный подход часто ошибочен и приводит к «нагромождению» юридических конструкций, что может навредить развитию и совершенствованию регулирования криптографической деятельности.

Значимый дисбаланс между ростом и усложнением отдельных информационных правоотношений и их местом в данном федеральном законе уже привел к его сложносистематизированному дополнению и изменению. Например, изначально содержащаяся в законе статья 15 «Использование информационно-телекоммуникационных сетей» была дополнена статьей 15.1, а затем эти статьи еще раз дополнили статьями 15.1-1 и 15.1-2. Это не единственный пример, но он позволяет наглядно продемонстрировать обоснованность доводов ученых о необходимости кардинального пересмотра процесса нормотворчества в сфере информационных отношений [11]. Одним из новых методов совершенствования информационного законодательства называют процесс кодификации, который предлагается реализовать через принятие Цифрового кодекса или Информационного кодекса [12, 13]. При этом концепция развития кодификации в данной сфере в большей мере нацелена на разработку и принятие узконаправленного Цифрового кодекса. В связи с отсутствием перспективы кодификации именно информационного законодательства оно развивается сегодня через принятие отдельных самостоятельных федеральных законов, регламентирующих оборот отдельных видов информации или создание и использование отдельных информационных технологий, информационных систем (например, ФЗ от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

В связи с этим, можно говорить, что совершенствование регулирования криптографической деятельности может осуществляться тремя способами:

1) через внесение изменений в существующий закон, что, как показывает опыт, не всегда эффективно;

2) через внесение соответствующего раздела в Информационный кодекс, что не возможно из-за отсутствия перспективы его принятия в среднесрочной перспективе;

3) через создание отдельного федерального закона, что представляется наиболее эффективным вариантом совершенствования регулирования криптографической деятельности в Российской Федерации.

Чтобы оценить возможность реализации третьего варианта развития законодательства о криптографической деятельности, необходимо оценить современное состояние законодательства о криптографии Российской Федерации.

Формирование законодательства о криптографии в Российской Федерации

Согласно актам нормативно-технического регулирования, криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации, а также прикладная инженерно-техническая дисциплина, которая занимается разработкой, анализом и обоснованием стойкости криптографических средств защиты информации от угроз со стороны противника, обеспечивая конфиденциальность, целостность, неотслеживаемость (см.: п. 3.15 ГОСТ Р 56875-2016. Национальный стандарт Российской Федерации. Информационные технологии системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий. Утвержден и введен в действие приказом Росстандарта от 26.02.2016 № 81-ст). Данный термин нельзя использовать в законодательстве, так как он сужает криптографическую деятельность до двух направлений: наука и прикладная инженерно-техническая дисциплина. Это не соответствует действительности, так как нормы, регламентирующие создание и использования СКЗИ охватывают более широкий круг общественных отношений. К таковым можно относить:

– отношения по созданию СКЗИ, включая регламентацию процесса сертификации;

– отношения по использованию СКЗИ;

– отношения по обороту СКЗИ, включая экспорт и импорт оборудования;

– отношения по оказанию услуг, сопряженных с криптографической деятельностью;

– отношения по контролю за криптографической деятельностью, а также иные управленческие отношения.

Полагаем, что предметом законодательства о криптографии также необходимо относить вопросы взаимодействия правоохранительных органов и криптографических информационных систем.

Данный перечень является гибким и может корректироваться вместе с развитием криптографической деятельности.

Закон о криптографической деятельности

Анализ складывающихся отношений в сфере криптографической деятельности, а также действующего открытого законодательства в данной сфере позволяет сделать вывод, что сегодня объективно необходим специальный федеральный закон, посвящённый криптографической деятельности. Его принятие во многом может способствовать развитию использования современных технологий защиты информации, в том числе квантовых коммуникаций.

Согласно сложившейся юридической практике значительная часть законов, регулирующих информационные отношения, не имеют деление на главы или разделы. Поэтому и федеральный закон о криптографической деятельности, на наш взгляд, целесообразно формировать без подобного разделения. Однако в целях систематизации информации и для удобства анализа в статье выделены две основные части проекта данного нормативного правового акта: общая и особенная. Это необходимо, чтобы структурировать нормы, изложив сначала, те, которые качаются общеправовых аспектов, а затем нормы, регулирующие отдельные виды криптографии или ее особенности.

1. Общая часть может включать статьи, посвященные:

– сфере действия законодательства о криптографии;

– системе законодательства о криптографии;

– принципам криптографической деятельности;

– полномочиям органов публичной власти в сфере криптографии;

– роли общественных организаций в сфере криптографии;

– правам и обязанностям субъектов криптографической деятельности, в том числе покупателям оборудования и потребителям работ и услуг в сфере криптографии;

– видам криптографии;

– положениям об экспорте и импорте СКЗИ;

– сертификации СКЗИ;

– лицензировании криптографической деятельности;

– вопросам использования криптографии в ходе ОРМ.

2. Особенная часть может включать статьи, посвященные:

– порядку определения случаев обязательного использования сертифицированной криптографии;

– особенностям использования симметричной и асимметричной криптографии;

– особенностям использования криптографии для аутентификации, включая технологии электронной подписи;

– особенностям использования квантовой криптографии;

– особенностям использования криптографии для проведения голосований в электронной форме;

– особенностям использования криптографии для создания и использования финансовых активов, включая криптовалюты;

– особенностям использования криптографии для дистанционного взаимодействия и управления объектами, включая беспилотный транспорт, IoT, умные счетчики;

– особенностям создания и использования методов криптоанализа.

Представляется, что содержание данных статей должно основываться на существующих нормах законодательства о криптографии, на институтах развития иных технологий цифровой экономики, показавших хороший результат, а также на лучших зарубежных и международных практиках, например, на Рекомендациях ОЭСР по формированию принципов государственной политики в области криптографии [14].

При разработке проекта федерального закона, посвященного криптографической деятельности, имеет первостепенное значение, чтобы эта работа способствовала формированию эффективной отечественной конкурентоспособной системы криптографии. Анализ процесса согласования нормативных правовых актов в информационной сфере показывает, что уполномоченные органы публичной власти, следуя стоящим перед ними задачам, стремятся вносить излишние запреты и ограничения, перестраховываясь от любых возможных рисков или пытаться минимизировать свои ресурсы, которые будет необходимо затратить на выполнение новых предписаний.

В целях недопущения подобного развития событий в сфере законодательства о криптографии представляется необходимым зафиксировать в официальном документе ключевые идеи (результаты), которые необходимо достичь органам публичной власти после его принятия. В качестве таковых можно выделить следующие:

1. Развитие рынка криптографии, под которым мы понимаем в первую очередь увеличение производства отечественного оборудования, сопряженного с ростом его качества. Жесткое регулирование отечественного криптографического рынка обеспечивает контроль за СКЗИ, включая запрет на допуск в Российскую Федерацию импортных СКЗИ. Подобные преимущества отечественным производителям снижают уровень конкуренции, а значит, влияют на качество отечественного оборудования. Изменить ситуацию без ущерба технологическому суверенитету можно двумя путями.

Частично открыть национальный рынок оборудования, например, путем введения института «гражданской криптографии». Это позволит обеспечить существование сегмента внутри страны с высоким уровнем конкуренции, что может привести к повышению качества отечественного оборудования. Следует отметить, что во многих государствах мира существует такое шифрование, например, в Канаде регулятор (Canadian Centre for Cyber Security) опубликовал в свободном доступе алгоритмы, которые следует применять для защиты конфиденциальной информации (Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information – ITSP.40.111). При этом не было ни одного прецедента системного взлома криптографических алгоритмов, что позволяет говорить о ее эффективности и безопасности.

При этом особый интерес вызывает опыт Китая, принявшего в 2023 году новый Закон о криптографии. Это первые значимые изменения в стране с 1999 года. Криптография в КНР стала классифицироваться на базовую, общую и коммерческую. Базовая криптография и общая криптография используются для защиты информации, составляющей государственную тайну, а коммерческая – для защиты иной информации ограниченного доступа. Среди новелл данного закона особо можно выделить следующие: информация о коммерческой криптографии перестала относиться к государственной тайне; добровольная сертификация коммерческого шифрования специализированной негосударственной организацией, кроме случаев их использования в критической информационной инфраструктуре; переход от «системы лицензирования» к «системе списков» при экспорте и импорте криптографического оборудования (ранее требовалось одобрение Национального управления криптографии). Теперь действуют «Список разрешений на импорт коммерческих средств шифрования» и «Список контроля за экспортом коммерческих средств шифрования», однако экспорт микросхем, оборудования для квантовой криптографии и криптографического испытательного оборудования требует отдельного разрешения.

Однако, на наш взгляд, этот вариант для отечественной криптографии имеет больше рисков, чем преимуществ. Есть высокая вероятность, что отечественные СКЗИ в сфере гражданской криптографии сместятся в сегмент «недорого оборудования», а импортные СКЗИ займут большую долю этого рынка. Поскольку отечественные компании не обладают экономическими ресурсами китайских коллег, то такой вариант развития нельзя признать оптимальным для России.

Более интересным выглядит вариант «экспансии» отечественных производителей СКЗИ на зарубежные рынки. Если перед государством стоит задача повысить качество оборудования через конкуренцию, то рациональнее выглядит стимулирование конкуренции на рынках других государств мира. Таким образом, можно говорить о целесообразности пересмотра в законодательстве о криптографии норм об экспорте СКЗИ, а также системы норм, обеспечивающих стимулирование данных процессов.

2. Внедрение в криптографическую деятельность элементов саморегулирования. Мы исходим из того, что рост рынка криптографии, указанный в качестве первой задачи закона о криптографии будет реализован, а значит, требуется пересмотр подходов к государственному управлению.

При его применении государство перестает осуществлять полный контроль каждого участника, что требует значительных ресурсов, а сосредотачивается на полном контроле саморегулируемых организаций и выборочном контроле их участников. При этом методе возникает интересный парадокс, саморегулируемые организации, выступая объектом жесткого контроля, внедряют к своим членам более жесткие требования, чем установленные законодательством, а также применяют более широкий перечень методов контроля. Таким образом, саморегулирование, при правильной организации, не только не снизит контроль за рынком криптографии, но даже позволит его усилить и диверсифицировать. Для этого необходимо закрепить права и обязанности саморегулируемых организаций в сфере криптографии, а также ответственность органов публичной власти за их работу.

При реализации этой задачи государству не потребуется создавать новые организации, так как в декабре 2022 г. уже создана Автономная некоммерческая организация «Национальный технологический центр цифровой криптографии», которую учредило Правительство Российской Федерации совместно с лидерами отрасли (АО «ИнфоТеКС», ООО «Код Безопасности» и ООО «Крипто-Про»). На международном уровне роль подобных организаций достаточно значима, например, работа Международной организации криптографических исследований сегодня значительным образом стимулирует исследования, а также обмен опытом по использованию разных методов шифрования.

3. Защита прав пользователей СКЗИ. Это один из самых сложных вопросов в сфере криптографии. Криптографическое сообщество уже обращало внимание на данную проблему, предлагая ввести институт независимых экспертов для оценки потребительских качеств оборудования [15]. Однако из данной идеи развить эффективную работающую модель не удалось. Исходя из сложившейся практики правоприменения, СКЗИ являются для пользователя часто черным ящиком, технические характеристики которого ничем не подтверждены. Регулятор дает сертификат, что оборудование соответствует государственным стандартам в области шифрования. Никаких иных характеристик сертификат не подтверждает. Данная проблема стоит особенно остро в публичных закупках. Если объективных характеристик оборудования нет или они не ясны, то государственные и муниципальные заказчики в ходе торгов должны выбирать самое дешевое оборудование, которое имеет сертификат. В итоге производители будут стремиться снизить стоимость, в том числе за счет качества комплектующих.

Помимо качества оборудования права потребителя требуют защиты в части определения случаев обязательного использования СКЗИ. В Российской Федерации отсутствует конкретный перечень ситуаций, когда у субъекта права возникает обязанность применять методы криптографической защиты информации. Многократные упоминания данной обязанности в разных законах и подзаконных актах разрешить данную проблему не могут, так как в большинстве случаев они оставляют решение этого вопроса за субъектом права.

Заключение

Развитие экономики данных способно привести Российскую Федерацию к ситуации, когда информация станет ее главным ресурсом, который нужно охранять надежнее, чем полезные ископаемые. Сегодня пока нет достаточно надежных методов защиты данных, которые бы стали заменой для криптографии.

В связи с этим не вызывает сомнений, что криптографическая деятельность долгое время будет ядром системы информационной безопасности в государстве.

Чтобы обеспечить технологический суверенитет в данной сфере, необходимо не только сохранить имеющийся потенциал отечественной криптографической школы, но и обеспечить ее долгосрочное развитие. Сегодня главным стимулом этого процесса является государство, которое в большинстве случаев выступает и заказчиком исследований и основным потребителем криптографического оборудования. Развитие данной отрасли во многом видится посредством повышения эффективности отечественного законодательства о криптографии.

Исследование показывает, что в России, как и в большинстве государств мира, отсутствует специальный закон о криптографии. Отдельные нормы, регламентирующие лицензирование деятельности, сертификацию оборудования, сферы использования шифрования, импорт и экспорт СКЗИ рассредоточен в различных нормативных правовых актах, которые нуждаются в качественной систематизации. Представляется, что решить данную проблему можно, инициировав разработку и принятие федерального закона, посвященного криптографической деятельности. В статье предложено содержание данного законопроекта, а также определены основные сферы, относящиеся к предмету его регулирования. Его принятие во многом будет способствовать развитию всей отечественной системы информационной безопасности, в том числе перспективных ее направлений, связанных с квантовыми коммуникациями.

Список источников

1. Евсиков К.С. Правовое регулирование поддержки отечественных производителей квантовых коммуникаций // Право и цифровая экономика. 2023. № 3. С. 11–19.
2. Полякова Т.А., Минбалеев А.В., Наумов В.Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. 2025. № 1. С. 160–173. doi: 10.31857/S1026945225010148
3. Полякова Т.А., Минбалеев А.В., Троян Н.А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С. 131–144. doi: 10.31857/S102694520025209-0
4. Полякова Т.А. Информационная безопасность в условиях построения информационного общества в России. М. : РПА Минюста России, 2007. 169 с.
5. Бачило И.Л., Полякова Т.А. На пути к обеспечению информационной безопасности – проблемы формирования государственной информационной политики и совершенствования законодательства // Государство и право. 2016. № 3. С. 66–77.
6. Дубоносов Е.С. Оперативно-розыскная деятельность : учебник для вузов. 8-е изд., перераб. и доп. М. : Юрайт, 2025. 399 с.
7. Minbaleev A., Zenin S., Evsikov K. Prospects for legal regulation of quantum communication // BRICS Law Journal. 2024. № 11 (2). P. 11–54. doi: 10.21684/2412-2343-2024-11-2-11-54
8. Минбалеев А.В., Ефремов А.А., Добробаба М.Б., Чубукова С.Г. Методы и подходы к регулированию формирующейся отрасли квантовых коммуникаций в условиях современного информационного общества // Информационное общество. 2024. № 4. С. 112–120. doi: 10.52605/16059921_2024_04_112
9. Минбалеев А.В., Берестнев М.А., Евсиков К.С. Обеспечение информационной безопасности оборудования добывающей промышленности в квантовую эпоху // Известия Тульского государственного университета. Науки о Земле. 2023. № 1-1. С. 567–584. doi: 10.46689/
2218-5194-2023-1-1-567-584.
10. Пономарева В.В., Розова Я.С. Протоколы квантового распределения ключей // Прикладная информатика. 2008. № 6 (18). С. 113–123.
11. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России // Государство и право. 2024. № 9. С. 166–179. doi: 10.31857/S1026945224090155
12. Полякова Т.А., Троян Н.А. Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2. С. 25–33. doi: 10.17803/2311-5998.2023.102.2.025-033
13. Полякова Т.А., Минбалеев А.В., Наумов В.Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 81–91. doi: 10.31857/S1026945224010087
14. Recommendation of the Council concerning Guidelines for Cryptography Policy // OECD. 2025. URL: https://legalinstruments.oecd.org/public/doc/115/115.en.pdf (дата обращения: 15.06.2025).
15. Академия информационных систем. Пресса о нас // Connect. 2011. № 5. URL: https://www.infosystems.ru/academy/pressa/connect-rossiyskiy-rynok-skzi/ (дата обращения: 15.06.2025).

References

1. Evsikov, K.S. (2023) Pravovoe regulirovanie podderzhki otechestvennykh proizvoditeley kvantovykh kommunikatsiy [Legal regulation of support for domestic producers of quantum communications]. *Pravo i tsifrovaya ekonomika*. 3. pp. 11–19.
2. Polyakova, T.A., Minbaleev, A.V. & Naumov, V.B. (2025) Sovremennyye prioritety razvitiya informatsionnogo prava: pravovoe obespechenie gosudarstvennogo suvereniteta i informatsionnoy bezopasnosti v informatsionnom prostranstve Rossii [Modern priorities of information law development: legal support of state sovereignty and information security in the information space of Russia]. *Gosudarstvo i pravo*. 1. pp. 160–173. doi: 10.31857/S1026945225010148
3. Polyakova, T.A., Minbaleev, A.V. & Troyan, N.A. (2023) Formirovaniye kultury informatsionnoy bezopasnosti grazhdan Rossiyskoy Federatsii v usloviyakh novykh vyzovov: publichno-pravovyye problemy. [Formation of information security culture of Russian Federation citizens under new challenges: public-law issues]. *Gosudarstvo i pravo*. 5. pp. 131–144. doi: 10.31857/S102694520025209-0
4. Polyakova, T.A. (2007) *Informatsionnaya bezopasnost' v usloviyakh postroyeniya informatsionnogo obshchestva v Rossii* [Information Security in the Context of Building the Information Society in Russia]. Moscow: RPA Minyusta Rossii.
5. Bachilo, I.L. & Polyakova, T.A. (2016) Na puti k obespecheniyu informatsionnoy bezopasnosti – problemy formirovaniya gosudarstvennoy informatsionnoy politiki i sovershenstvovaniya zakonodatel'stva [On the way to ensuring information security – problems of state information policy formation and legislation improvement]. *Gosudarstvo i pravo*. 3. pp. 66–77.

6. Dubonosov, E.S. (2025) *Operativno-rozysknaya deyatel'nost'* [Operative-Search Activity]. 8th ed. Moscow: Yurayt.
7. Minbaleev, A., Zenin, S. & Evsikov, K. (2024) Prospects for legal regulation of quantum communication. *BRICS Law Journal*. 11 (2). pp. 11–54. doi: 10.21684/2412-2343-2024-11-2-11-54
8. Minbaleev, A.V. et al. (2024) Metody i podkhody k regulirovaniyu formiruyushcheysya otrasli kvantovykh kommunikatsiy v usloviyakh sovremennogo informatsionnogo obshchestva [Methods and approaches to regulation of the emerging quantum communications industry in the context of modern information society]. *Informatsionnoye obshchestvo*. 4. pp. 112–120. doi: 10.52605/16059921_2024_04_112
9. Minbaleev, A.V., Berestnev, M.A. & Evsikov, K.S. (2023) Obespecheniye informatsionnoy bezopasnosti oborudovaniya dobyvayushchey promyshlennosti v kvantovuyu epokhu [Ensuring information security of extractive industry equipment in the quantum era]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Nauki o Zemle*. 1-1. pp. 567–584. doi: 10.46689/2218-5194-2023-1-1-567-584
10. Ponomareva, V.V. & Rozova, Ya.S. (2008) Protokoly kvantovogo raspredeleniya klyuchey [Quantum key distribution protocols]. *Prikladnaya informatika*. 6 (18). pp. 113–123.
11. Polyakova, T.A., Minbaleev, A.V. & Krotkova, N.V. (2024) Transformatsiya nauki informatsionnogo prava i informatsionnogo zakonodatel'stva: novyy etap v usloviyakh nauchno-tekhnologicheskogo razvitiya Rossii [Transformation of information law science and information legislation: new stage in the context of scientific and technological development of Russia]. *Gosudarstvo i pravo*. 9. pp. 166–179. doi: 10.31857/S1026945224090155
12. Polyakova, T.A. & Troyan, N.A. (2023) Aktual'nyye problemy sistematizatsii zakonodatel'stva Rossii pod vliyaniyem tsifrovykh tekhnologiy v period tsifrovoy transformatsii [Current issues in systematization of Russian legislation under influence of digital technologies in the period of digital transformation]. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA)*. 2. pp. 25–33. doi: 10.17803/2311-5998.2023.102.2.025-033
13. Polyakova, T.A., Minbaleev, A.V. & Naumov, V.B. (2024) K voprosu o kodifikatsii informatsionnogo zakonodatel'stva v usloviyakh tsifrovoy transformatsii [On the issue of codification of information legislation in the conditions of digital transformation]. *Gosudarstvo i pravo*. 1. pp. 81–91. doi: 10.31857/S1026945224010087
14. OECD (2025) *Recommendation of the Council concerning Guidelines for Cryptography Policy*. [Online] Available from: https://legalinstruments.oecd.org/public/doc/115/115.en.pdf (Accessed: 15.06.2025).
15. Akademiya informatsionnykh sistem [Academy of Information Systems]. (2011) Pressa o nas [Press about Us]. *Connect*. 5. [Online] Available from: https://www.infosystems.ru/academy/pressa/connect-rossiyskiy-rynok-skzi/ (Accessed: 15.06.2025).

Информация об авторах:
Минбалеев А.В. – д-р юрид. наук, зав. кафедрой информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) (Москва, Россия). E-mail: avminbaleev@msal.ru
Евсиков К.С. – канд. юрид. наук, доцент, зав. кафедрой государственного и административного права Тульского государственного университета (Тула, Россия); доцент кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) (Москва, Россия). E-mail: aid-ltd@yandex.ru

Авторы заявляют об отсутствии конфликта интересов.

Information about the authors:
A.V. Minbaleev, Dr. Sci. (Law), head of the Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (Moscow, Russian Federation). E-mail: avminbaleev@msal.ru
K.S. Evsikov, Cand. Sci. (Law), docent, head of the Department of State and Administrative Law, Tula State University (Tula, Russian Federation); associate professor, Kutafin Moscow State Law University (Moscow, Russian Federation). E-mail: aid-ltd@yandex.ru

The authors declare no conflicts of interests.

Статья поступила в редакцию 25.07.2025;
одобрена после рецензирования 17.09.2025; принята к публикации 30.09.2025.

The article was submitted 25.07.2025;
approved after reviewing 17.09.2025; accepted for publication 30.09.2025.