

УДК 343

DOI: 10.34670/AR.2026.36.38.050

Уголовная политика в сфере обеспечения цифрового суверенитета

Пекарева Виктория Владимировна

Магистрант,
юридический факультет,
Российский государственный
педагогический университет им. А.И. Герцена,
191186, Российская Федерация,
Санкт-Петербург, набережная реки Мойки, 48;
e-mail: viktoria.pekareva@yandex.ru

Аннотация

Особая значимость цифровой среды, в частности сети «Интернет», как объекта уголовно-правовой охраны предопределяется исключительным социально-стратегическим статусом, а также специфическими техническими характеристиками. Исследование направлено на демонстрацию и доказательность того, что «соблазнительный» и справедливо отстаиваемый многими учеными, в контексте рассмотрения образующих понятийного аппарата цифрового суверенитета, баланс между механизмами государственного контроля для обеспечения национальной безопасности, устойчивости к внешним и внутренним дестабилизирующим воздействиям и открытостью, свободой выбора веб-ресурсов гражданами, их использованием ими, выглядит как утопическая идея и стремление к идеалу, однако вполне возможен, хоть и вопреки всему трудно реализуем. Любая попытка зафиксировать эту точку равновесия неизбежно сталкивается с очевидным противоречием между трансграничной, децентрализованной природой самой сети «Интернет» (цифровая среда развивается по принципу самоорганизации, сетевых эффектов и постоянного технологического усложнения, совершенствуясь) и классическими механизмами государственно-правового регулирования. Однако в научной работе не просто рассматривается упомянутый компромисс и его значение, что характеризует цифровой суверенитет в одной из идеальных форм, но и отстаивается мнение о достижении равновесия через защиту функционального целого информационно-телекоммуникационной сети «Интернет» без ущерба правам, интересам граждан. Отрицание необходимости подобного свидетельствует не о стремлении к свободе, а о безответственном отношении к реализации концепции, в особенности, уголовно-правовой, охраны цифровой дееспособности государства и общества.

Для цитирования в научных исследованиях

Пекарева В.В. Уголовная политика в сфере обеспечения цифрового суверенитета // Вопросы российского и международного права. 2026. Том 16. № 7А. С. 483-491. DOI: 10.34670/AR.2026.36.38.050

Ключевые слова

Цифровой суверенитет, интернет, устойчивость, целостность, конфиденциальность, информационная безопасность, уголовно-правовая охрана, цифровая среда, информационно-телекоммуникационная сеть, суверенизация интернета, преступления в сфере компьютерной информации.

Введение

Пока есть государство, нет свободы.

Когда будет свобода, не будет государства.

Владимир Ленин

С одной стороны, уголовный закон призван обеспечивать стабильность правопорядка, системность и предсказуемость правоприменения (его единообразие). С другой стороны, под воздействием динамично меняющихся общественных отношений, медийного, политического дискурса, мультипликативной в своем положительном и негативном развитии цифровой среды, а также актуальных государственных запросов уголовно-правовые институты нередко подвергаются точечным преобразованиям.

Описанное характеризует часть того, из чего складывается уголовная политика. При всей ее парадоксальности в сфере гарантии информационной и обеспечения национальной безопасности она выступает универсальным инструментарием, выстраивающем свои методологические корни на интегративном и междисциплинарном подходе, что значительно расширяет возможность противодействия киберпреступности. Однако невозможно не учесть излишний субъективизм, приводящий к оценочным суждениям, искажая объективный смысл уголовно-правовой охраны, заложенный реальными потребностями защиты информационного пространства.

Основная часть

В актуальной юридической парадигме информационно-телекоммуникационная сеть «Интернет» перестает рассматриваться исключительно в качестве нейтрального коммуникационного пространства или прикладного инструмента обмена данными. В современных реалиях она справедливо представляет собой специфическую сложно структурированную децентрализованную техническую среду и экосистему социотехнических отношений, где цифровые возможности выступают одновременно детерминантой общественного прогресса и пространством потенциальной криминальной экспансии, ввиду чего проблема её защиты неразрывно связывается с вопросами цифрового суверенитета и обеспечения национальной безопасности. П.Н. Астапенко вносит существенный вклад в понимание текущей «картины» того, что из себя представляет интернет-пространство, а именно это та среда, по его обоснованному мнению, которая по своей роли и значению не уступает реальному пространству, в отношении которого действуют принципы и правила государственного суверенитета. Оно не имеет физических границ, однако де-факто поделено между социальными сетями, мессенджерами, сервисами и другими интернет-ресурсами. Каждый интернет-ресурс имеет собственную власть, роль которой, без преувеличения,

аналогична публичной власти, реализующей свое суверенное право на конкретной территории, квази-суверенитет [Астапенко, 2022]. В данном контексте исследовательский фокус смещается с единичных эпизодов хищений или частных случаев мошенничества на качественную трансформацию преступности, адаптирующей сетевое пространство в качестве способа собственного функционирования, воспроизводства и эскалации. Подобный процесс создает угрозу для устойчивости функционирования веб-ресурсов, их доступности, стабильных информационных обменов, конфиденциальности сведений компаний и граждан, безопасности критической информационной инфраструктуры, что подрывает доверие к цифровым ресурсам и техническим средствам, а также дестабилизирует управляемость социальных процессов в целом. Неспроста С.И.Коданева заостряет внимание на технический аспект, а именно на сложность цифровой среды, которая является многослойной и включает в себя физическую инфраструктуру, технические стандарты, программы (алгоритмы), включая платформы, и размещаемый на них или с их помощью контент, что эти слои могут контролироваться различными субъектами, что создаёт проблемы юрисдикции: пакет данных из ЕС, передаваемый по подводному кабелю, принадлежащему американской компании, обрабатывается в индийском дата-центре с помощью платформы, принадлежащей Китаю [Коданева, 2025].

С технологической точки зрения неспроста В. А. Никонов подчеркивает необходимость развития национальной цифровой инфраструктуры и внедрения передовых технологий, включая разработку национальных операционных систем и инструментов для работы с большими данными, затрагивая вопросы защиты национальной информационной среды от внешних угроз, таких как кибератаки и цифровой шпионаж [Никонов и др., 2021]. Нельзя не признать справедливость тезиса авторов - О.А. Кожевниковой и А.В. Нечкина о том, что «каждое государство, объявляя себя суверенным, стремится любыми доступными способами в рамках норм международного и национального права защитить свой суверенитет от какого-либо влияния со стороны других государств, потому как в противном случае оно рискует лишиться той или иной части своих суверенных прав, что ведет к изменению его правового статуса» [Кожевников, Нечкин, 2021]. В настоящее время особую значимость приобретает новое осмысление фундаментальных понятий теории государства и права. Эволюция общественных отношений способствует накоплению и обновлению знаний о правовой действительности [Мотова, 2026]. Придерживаясь позиции исследователей Г.А. Адамяна, О.В. Биктасова, А.А.Вихрова, М.В.Сальникова, что сущность суверенитета - это прежде всего социально-политические и правовые отношения и это не свойство, не состояние власти, которые характеризуют лишь различные стороны качества власти и государства, что они выражают и характер, и качество политико-правовых отношений, которые составляют внутреннюю стержневую основу любого общества, государства и любой власти, их сущность [Вихров и др., 2005], приступим к рассмотрению цифрового суверенитета, прежде чем перейти к его непосредственному анализу в контексте уголовно-правовых отношений.

Очевидно, что рассмотрения вопроса о том, как правильно выстраивать государственный механизм в области цифрового суверенитета, и выбора в определении понятия «цифровой суверенитет» преимущественного предпочтения из двух крайностей между приоритетом порядка и безопасности, ассоциируемых с суверенитетом, и проявлением субъектной воли, выраженным в категории свободы было чем-то невозможным. Этому и уделено внимание в мысли, отраженной в эпиграфе исследования. Однако с полным пониманием неизбежности упоминания ключевой дискуссии многих ученых, отстаивающих ту или иную позицию,

эпиграф, который обычно формирует смысловое наполнение содержания текста или его части, отражая субъектную позицию автора по отношению к последующему изложению, представляло собой всего лишь диалектическим приемом, который мгновенно трансформирует проблематику суверенитета из области рутинного политологического анализа в контекст напряженного дискурса относительно приоритетности институциональной безопасности и порядка перед концептом свободной воли. Использованный маневр носил исключительно вводный характер, имея своей целью привлечение внимания к корректной интерпретации сути вопроса о том, какой именно, по нашему мнению, цифровой суверенитет защищаем и чем он является. Это не только инструмент защиты, но и ресурс долгосрочной устойчивости и культурного влияния. В рамках подобных рассуждений произнесённые слова министром цифрового развития, связи и массовых коммуникаций Российской Федерации Максудом Шадаевым в ходе международного форума по практической кибербезопасности «Positive Hack Days» 2025 года играют по-другому, наделяясь специфической семантической значимостью: «Цифровой суверенитет - это прежде всего способность государства обеспечить защиту интересов своих граждан и собственной информационной инфраструктуры независимо от внешнеполитических обстоятельств и санкционного давления». Концепция цифрового суверенитета, развиваемая на национальном уровне, является объективной реакцией на неспособность международного права защитить государства от гибридных угроз [Шарафиев, 2026].

Соответствующее понимание, основанное на публично-правовых аспектах и предложенное А.С.Агафоновым, позволяет сложить верное впечатление о сущности цифровой суверенности государства (цифрового суверенитета) как способности государства самостоятельно создавать и использовать в различных сферах деятельности собственные средства вычислительной техники, программы для электронных вычислительных машин и базы данных, которые являются критически важными для обеспечения благосостояния населения государства, его национальной безопасности и конкурентоспособности национальной экономики, а также возможность государства определять и проводить самостоятельную внутреннюю и внешнюю политику в информационной сфере [Агафонов, 2026]. Охранительное воздействие уголовно-правовых норм должно быть направлено не на ограничение свободной цифровой активности правомерных субъектов, а на криминализацию и наказание деяний, сопряжённых с деструктивным вмешательством в функционирование цифровых систем и ресурсов, нарушающим их целостность, устойчивость, конфиденциальность и доступность, что создает угрозу национальной безопасности и суверенитету в цифровом пространстве, а также представляет потенциальную опасность для ценностных ориентиров и социокультурной идентичности каждого гражданина. Данная модель полностью соотнобразуется с пониманием цифрового суверенитета как способности государства суверенно регулировать цифровые ресурсы, гарантируя их защищенность от внешних посягательств и внутренних деструктивных факторов.

Относительно недавними нововведениями в уголовное законодательство были нормы, закрепленные в статьях 274.3, 274.4 и 274.5 УК РФ, представляющие собой составляющие единой уголовно-правовой политики в плане недопущения неправомерной эксплуатации абонентских терминалов маршрутизации трафика или виртуальных телефонных станций, равно как и организации деятельности по передаче абонентских номеров с нарушением установленных регламентов либо сведений, необходимых для идентификации и аутентификации пользователей при получении доступа к функционалу информационных ресурсов. Наряду с этим, пополнен и списокотягчающих обстоятельств п.ф ст.63 УК РФ

(совершение преступления с использованием программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен)). Многообразие платформ и сервисов IP-телефонии обуславливает необходимость обладания специализированными знаниями и применения соответствующих инструментов при проведении оперативно-розыскных мероприятий. VoIP, GSM-шлюзы и SIM-банки представляют собой полезные технологические решения для интеграции сетей VoIP и GSM, которые превращаются в мощный инструмент реализации преступных схем. Однако не всегда вносимые изменения как корректирующие, так и вводимые нечто новое в УК РФ способны совершенствовать механизмы правового регулирования в информационной сфере. Русскевич Е. А., комментируя одну из новелл уголовного права, объективно замечает, что предложенная законодательная модель ответственности представителей операторов связи за нарушения в области эксплуатации технических средств противодействия угрозам (ст. 274.2 УК РФ) не представляется оптимальной: уязвимым является подход к описанию административно-преюдициальных признаков состава; возможность уголовно-правовой реакции на конкретный инцидент появляется не в связи с наступлением тех или иных общественно опасных последствий, а лишь при третьем задокументированном нарушении [Русскевич, 2023]. По мнению Русскевича Е. А., в данной норме УК РФ законодатель допускает не вполне удачное использование терминологии [Русскевич, 2023].

Несмотря на то, что правовое регулирование информационной безопасности, в частности, привлечение к уголовной ответственности за преступления в информационной сфере, в последнее время претерпело значительные улучшения, оно по-прежнему не удовлетворяет потребностям времени и на сегодняшний день существует немало пробелов в законодательстве, регулирующем вопросы привлечения к уголовной ответственности в сфере информации [Вепренцева, 2025]. Кроме того, заметно, что уголовный закон использует конструкции, заимствованные из информационного, административного и гражданского права, без их адаптации к уголовно-правовому контексту, требующему повышенной точности и определенности. Это противоречит принципу формальной определенности уголовного закона. Также, обращает на себя особое внимание технологическая нейтральность формулировок, изначально рассматриваемая многими как достоинство, оборачивается неопределенностью и несоответствием действительности, сложностями правоприменения. Под одно понятие могут подпадать принципиально разные с технической и социальной точки зрения явления. Отсутствие легальных дефиниций или наличие их в устаревшем виде (компьютерная информация тому одно из очевидных доказательств), а также их чрезмерная общность перекладывает бремя толкования на правоприменителя, который не всегда обладает необходимыми техническими знаниями и возможностями [Пекарева, 2026].

Наряду с прямым внесением изменений в основополагающий источник уголовного права, его нормы, в частности, объективную сторону закрепленных составов преступлений, детализируются посредством иных нормативно-правовых актов, что обязывает для установления факта совершения преступления, а также для уголовно-правовой оценки противоправного поведения в области устойчивости и безопасности информационно-телекоммуникационной сети «Интернет» и сетей связи обратиться к правилам и требованиям, без которых перечисленное не представляется возможным. Речь идет в первую очередь об относительно недавно изменившихся и принятых следующих нормативно-правовых актах:

- Постановление РФ от 30.08.2025 №1333, которым обновлены и установлены обязательные правила установки, эксплуатации и модернизации технических средств противодействия

угрозам для обеспечения целостности, безопасности и устойчивости работы сети «Интернет» и сети связи общего пользования операторами связи;

- Постановление Правительства РФ от 15.01.2024 №4, регулирующее установку, эксплуатацию и модернизацию технических средств противодействия угрозам в точках обмена трафиком: за эти процессы отвечают радиочастотная служба и владельцы точек обмена трафиком. В постановлении прописан порядок взаимного обмена и обновления информации между ними (подача и ответ на запросы, сроки и форма взаимодействия), требования к техническим характеристикам средств, строгие сроки для обмена информацией и уведомления о событиях (установка, модернизация, изменения подключения), а также оформление актов передачи и возврата технических средств.

Нужно при этом учесть, что это не единичные нормативно-правовые акты, к которым необходимо обращаться при квалификации содеянного или разбора уголовно-правовых норм, поскольку составы преступлений, закрепленные в главе 28 УК РФ, преимущественно бланкетного характера, в особенности, все новеллы, появляющиеся в последнее время, при анализе которых обойтись без сторонних законов и подзаконных актов кроме уголовного кодекса никоим образом не возможно, да и нецелесообразно. Несмотря на очевидные результаты в развитии законодательства, регулирующего ответственность за компьютерные преступления, по-прежнему способствуют стремительному развитию безнаказанной противоправной деятельности современных компьютерных злоумышленников. В то же время, оправдываются прогнозы многих ученых о том, что рост преступлений, связанных с компьютерной информацией, будет продолжаться, в связи с чем особое значение имеет готовность внутригосударственного уголовного законодательства к активному совершенствованию современной преступной деятельности [Берова, 2020].

Е.В.Кунц своими рассуждениями замечает справедливую взаимосвязь, которая не раз подчеркивалась в статье, а именно, что пока все опции исполнения и интерпретации национального законодательства не будут полностью использованы, трудно определить, на какие средства нужно соглашаться на международном уровне. Принцип территориальности дает возможность странам навязывать свой суверенитет информационной инфраструктуре, находящейся в пределах их территории, или действовать в соответствии с их юрисдикцией. Ответственность государства за безопасность своих сетей поддерживается принятыми международными принципами невмешательства и суверенитета [Кунц, 2025].

Министерством цифрового развития Российской Федерации представило проект доктрины, направленной на пресечение преступлений и иных правонарушений, совершаемых с применением информационных технологий. Стратегический документ рассчитан на период до 2035 года и вынесен на публичное обсуждение, закрепляя понятийно-категориальный аппарат, определяющий технологический и нормативно-правовой инструментарий государственной политики. В нормативный оборот вводятся дефиниции «антифрод-мер» как совокупности правовых, технических и организационных механизмов выявления и предотвращения правонарушений, «антифрод-системы», «Платформа» (Федеральный закон от 1 апреля 2025 г. №41-ФЗ и Постановление Правительства РФ от 27 февраля 2026 г. №200) в качестве специализированной государственной информационной системы, а также концепты «цифрового следа» и «электронного (цифрового) доказательства», составляющие основу процессуальной деятельности. Кроме того, нормативный акт оперирует понятиями «цифровая гигиена», «цифровая грамотность» и «противоправная инфраструктура». Ключевым элементом создаваемой архитектуры становится Платформа, функционирующая с 1 марта 2026 года:

данный институт объединяет правоохранительные органы, Банк России, финансовые организации, операторов связи и цифровые платформы в единую интеграционную среду, обеспечивающую формирование так называемого «цифрового иммунитета». Формирование последнего у государства и общества предполагает смещение уголовно-правового фокуса с репрессивного реагирования на упреждающую нейтрализацию системных угроз. Уголовно-правовая политика в рассматриваемой области будет выступать не инструментом карательного воздействия, а механизмом селективного сдерживания, строго ориентированным на нейтрализацию деструктивных цифровых факторов. Базовым ориентиром данного подхода является формирование системы цифровой защищенности, а не установление надзора, в силу чего заметна направленность в большей степени на блокирование конкретных угроз, а не на введение всеобщих запретов.

Заключение

Резюмируя вышеизложенное, ключевым становится тезис, что при стремлении к достижению безупречной своевременной охраны информационно-телекоммуникационной сети «Интернет», ее пользователей, компаний, государства, обеспечения стабильности и устойчивости интернет-ресурсов, противодействия реализации противоправного поведения в сети и связанных с ней преступлений, а также защиты разноплановой информации во всех сферах жизнедеятельности граждан не должно сопровождаться обесцениванием свободы доступа к веб-платформам, их использованием, не противоречащим отечественным законодательством, права на публикацию, поиск сведений, равно как и приводить к положению, при котором государство и отдельный гражданин, в частности, становится объектом чужой воли, навязанной иностранными механизмами, пренебрегая уже не просто своими ценностями, но и независимостью. Кроме того, необходимо внимательно относиться к техническим характеристикам внедряемых инструментов, решений, административных и уголовных норм права, а также учитывать, что избыточные или недостаточно проработанные ограничения способны не только снизить эффективность проводимой политики, но и вызвать отторжение у пользователей, подтолкнув их к использованию альтернативных каналов и обходных технологий.

Библиография

1. Агафонов, А. С. Цифровая суверенность государства в российском праве / А. С. Агафонов // Сибирское юридическое обозрение. – 2026. – № 2. – URL: <https://cyberleninka.ru/article/n/tsifrovaya-suverennost-gosudarstva-v-rossiyskom-prave-1>.
2. Астапенко, П. Н. Цифровой суверенитет как условие реализации государственного суверенитета в интернет-эпоху / П. Н. Астапенко // Закон и право. – 2022. – № 9. – С. 27–33. – DOI 10.24412/20733313_2022_9_27.
3. Берова, Д. М. Правовое регулирование ответственности за преступления в сфере компьютерной информации: проблемы и перспективы развития / Д. М. Берова // Пробелы в российском законодательстве. – 2020. – Т. XIII, № 3. – С. 121–123.
4. Вепренцева, Т. А. Информационное право. Ответственность в информационной сфере : учебное пособие / Т. А. Вепренцева. – Тула : Тул. ин-т (филиал) ВГУЮ (РПА Минюста России), 2025. – 131 с.
5. Вихров, А. А. Понятие и сущность суверенитета / А. А. Вихров, М. В. Сальников, Г. А. Адамян, О. В. Биктасов // Вестник Санкт-Петербургского университета МВД России. – 2005. – № 3. – URL: <https://cyberleninka.ru/article/n/ponyatie-i-suschnost-suvereniteta>.
6. Кожевников, О. А. Некоммерческие организации – иностранные агенты: опыт России и других государств СНГ / О. А. Кожевников, А. В. Нечкин // Вестник Томского государственного университета. – 2021. – № 471. – С. 242–249.
7. Коданева, С. И. Цифровой суверенитет как новая правовая концепция / С. И. Коданева // Московский юридический журнал. – 2025. – № 4. – С. 14–28. – DOI 10.18384/2949-513X-2025-4-14-28.

8. Кунц, Е. В. Противодействие современным киберпреступлениям / Е. В. Кунц // Российско-азиатский правовой журнал. – 2025. – № 1. – С. 97–104. – DOI 10.14258/ralj(2025)1.15.
9. Мотова, Е. А. Правовая природа технологического суверенитета в условиях новой социальной реальности / Е. А. Мотова // Академический юридический журнал. – 2026. – Т. 27, № 2(104). – С. 271–279. – DOI 10.17150/1819-0928.2026.27(2).271-279.
10. Никонов, В. А. Цифровой суверенитет современного государства: содержание и структурные компоненты (по материалам экспертного исследования) / В. А. Никонов, А. С. Воронов, В. А. Сажина, С. В. Володенков, М. В. Рыбакова // Вестник Томского государственного университета. Философия. Социология. Политология. – 2021. – № 60. – С. 206–216.
11. Пекарева, В. В. Понятийный аппарат в уголовно-правовой охране информационной безопасности: содержание и проблемы толкования / В. В. Пекарева // Вопросы российского и международного права. – 2026. – Т. 16, № 2-1. – С. 591–597. – DOI 10.34670/AR.2026.68.49.067.
12. Русскевич, Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности / Е. А. Русскевич // Journal of Digital Technologies and Law. – 2023. – № 1(3). – С. 650–672. – DOI 10.21202/jdtl.2023.28.
13. Шарафиев, К. И. Правовые и политические аспекты обеспечения национальной безопасности в условиях гибридных угроз / К. И. Шарафиев // Гуманитарный научный вестник. – 2026. – № 4. – С. 102–109. – DOI 10.5281/zenodo.19734915.

Criminal Policy in the Sphere of Ensuring Digital Sovereignty

Viktoriya V. Pekareva

Master's Student,
Faculty of Law,

Herzen State Pedagogical University of Russia,

191186, 48, Moyki river embankment, Saint Petersburg, Russian Federation;

e-mail: viktoriya.pekareva@yandex.ru

Abstract

The particular significance of the digital environment, in particular the Internet, as an object of criminal law protection is predetermined by its exceptional social-strategic status, as well as by specific technical characteristics. The study is aimed at demonstrating and proving that the "seductive" and justly defended by many scholars, in the context of considering the constituent conceptual apparatus of digital sovereignty, balance between the mechanisms of state control for ensuring national security, resilience to external and internal destabilizing influences, and openness, citizens' freedom to choose web resources and their use of them, looks like a utopian idea and a striving for an ideal, yet is quite possible, although contrary to everything difficult to implement. Any attempt to fix this point of equilibrium inevitably encounters an obvious contradiction between the transborder, decentralized nature of the Internet itself (the digital environment develops according to the principle of self-organization, network effects, and constant technological complication, improving itself) and the classical mechanisms of state-legal regulation. However, the scientific work not only examines the aforementioned compromise and its significance, which characterizes digital sovereignty in one of its ideal forms, but also defends the opinion that equilibrium is achievable through the protection of the functional whole of the information and telecommunications network "Internet" without prejudice to the rights and interests of citizens. The denial of the necessity of such protection testifies not to a striving for freedom, but to an irresponsible attitude toward the implementation of the concept, especially the criminal law protection, of the digital capability of the state and society.

For citation

Pekareva V.V. (2026) Ugolovnaya politika v sfere obespecheniya tsifrovogo suvereniteta [Criminal Policy in the Sphere of Ensuring Digital Sovereignty]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (7A), pp. 483-491. DOI: 10.34670/AR.2026.36.38.050

Keywords

Digital sovereignty, Internet, resilience, integrity, confidentiality, information security, criminal law protection, digital environment, information and telecommunications network, sovereignization of the Internet, computer information crimes.

References

1. Agafonov, A. S. (2026) Tsifrovaya suverennost' gosudarstva v rossiyskom prave [Digital sovereignty of the state in Russian law]. *Sibirskoye yuridicheskoye obozreniye*, (2). <https://cyberleninka.ru/article/n/tsifrovaya-suverennost-gosudarstva-v-rossiyskom-prave-1>
2. Astapenko, P. N. (2022). Tsifrovoy suverenitet kak usloviye realizatsii gosudarstvennogo suvereniteta v internet-epokhu [Digital sovereignty as a condition for the implementation of state sovereignty in the Internet era]. *Zakon i pravo*, (9), 27–33. https://doi.org/10.24412/20733313_2022_9_27
3. Berova, D. M. (2020). Pravovoye regulirovaniye otvetstvennosti za prestupleniya v sfere komp'yuternoy informatsii: problemy i perspektivy razvitiya [Legal regulation of liability for crimes in the field of computer information: problems and prospects of development]. *Probely v rossiyskom zakonodatel'stve*, *13*(3), 121–123.
4. Kodaneva, S. I. (2025). Tsifrovoy suverenitet kak novaya pravovaya kontseptsiya [Digital sovereignty as a new legal concept]. *Moskovskiy yuridicheskiy zhurnal*, (4), 14–28. <https://doi.org/10.18384/2949-513X-2025-4-14-28>
5. Kozhevnikov, O. A., & Nechkin, A. V. (2021). Nekommercheskiye organizatsii – inostrannyye agenty: opyt Rossii i drugikh gosudarstv SNG [Non-profit organizations – foreign agents: the experience of Russia and other CIS countries]. *Vestnik Tomskogo gosudarstvennogo universiteta*, (471), 242–249.
6. Kunts, E. V. (2025). Protivodeystviye sovremennym kiberprestupleniyam [Countering modern cybercrimes]. *Rossiysko-aziatskiy pravovoy zhurnal*, (1), 97–104. [https://doi.org/10.14258/ralj\(2025\)1.15](https://doi.org/10.14258/ralj(2025)1.15)
7. Motova, E. A. (2026) Pravovaya priroda tekhnologicheskogo suvereniteta v usloviyakh novoy sotsial'noy real'nosti [The legal nature of technological sovereignty in the conditions of a new social reality]. *Akademicheskii yuridicheskiy zhurnal*, *27*(2), 271–279. [https://doi.org/10.17150/1819-0928.2026.27\(2\).271-279](https://doi.org/10.17150/1819-0928.2026.27(2).271-279)
8. Nikonov, V. A., Voronov, A. S., Sazhina, V. A., Volodenkov, S. V., & Rybakova, M. V. (2021). Tsifrovoy suverenitet sovremennogo gosudarstva: sodержaniye i strukturnyye komponenty [Digital sovereignty of the modern state: content and structural components]. *Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya*, (60), 206–216.
9. Pekareva, V. V. (2026) Ponyatiynyy apparat v ugolovno-pravovoy okhrane informatsionnoy bezopasnosti: sodержaniye i problemy tolkovaniya [Conceptual apparatus in the criminal law protection of information security: content and problems of interpretation]. *Voprosy rossiiskogo i mezhdunarodnogo prava*, *16*(2-1), 591–597. <https://doi.org/10.34670/AR.2026.68.49.067>
10. Russkevich, E. A. (2023). Narusheniye pravil tsentralizovannogo upravleniya tekhnicheskimi sredstvami protivodeystviya ugrozam informatsionnoy bezopasnosti [Violation of the rules of centralized management of technical means of countering information security threats]. *Journal of Digital Technologies and Law*, *1*(3), 650–672. <https://doi.org/10.21202/jdtl.2023.28>
11. Sharafiev, K. I. (2026) Pravovyye i politicheskiye aspekty obespecheniya natsional'noy bezopasnosti v usloviyakh gibridnykh ugroz [Legal and political aspects of ensuring national security in the context of hybrid threats]. *Gumanitarnyy nauchnyy vestnik*, (4), 102–109. <https://doi.org/10.5281/zenodo.19734915>
12. Veprentseva, T. A. (2025). *Informatsionnoye pravo. Otvetstvennost' v informatsionnoy sfere* [Information law. Responsibility in the information sphere]. Tula Institute (branch) of the All-Russian State University of Justice.
13. Vikhrov, A. A., Salnikov, M. V., Adamyan, G. A., & Biktasov, O. V. (2005). Ponyatiye i sushchnost' suvereniteta [The concept and essence of sovereignty]. *Vestnik Sankt-Peterburgskogo universiteta MVD Rossii*, (3). <https://cyberleninka.ru/article/n/ponyatie-i-suschnost-suvereniteta>