- НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ -

Дата поступления рукописи в редакцию: 14.07.2026 г. DOI: 10.24412/2782-3830-2026-8-39-48
Дата принятия рукописи в печать: 04.08.2026 г.

РАДЫГИН Евгений Владимирович,
кандидат технических наук, доцент кафедры гуманитарных и социально-экономических дисциплин Северо-Западного филиала Российского государственного университета правосудия,
e-mail: radyginev@mail.ru

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОГО СУВЕРЕНИТЕТА: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА РОССИИ И КИТАЯ

Аннотация. *В статье проведен комплексный теоретико-правовой анализ понятия «информационный суверенитет» в контексте современной геополитической нестабильности и ускоренной цифровизации. Выявлены ключевые проблемы законодательного регулирования цифровых границ в Российской Федерации. На основе сравнительно-правового метода исследованы модели обеспечения информационного суверенитета Китая и России и предложены рекомендации по формированию оптимальной гибридной модели информационного суверенитета для России.*

Ключевые слова: *информационный суверенитет; Китайская Народная Республика, Российская Федерация, сравнительно-правовой анализ; критическая информационная инфраструктура; юридическая ответственность.*

RADYGIN Evgeny Vladimirovich,
Candidate of Technical Sciences, Associate Professor of the Department of Humanities and Socio-Economic Disciplines of the North-West Branch of the Russian State University of Justice

ENSURING INFORMATION SOVEREIGNTY: A COMPARATIVE LEGAL ANALYSIS OF THE LEGISLATION OF RUSSIA AND CHINA

Annotation. *The article provides a comprehensive theoretical and legal analysis of the concept of "information sovereignty" in the context of contemporary geopolitical instability and accelerated digitalization. The study identifies key challenges in the legislative regulation of digital borders in the Russian Federation. Utilizing a comparative legal method, the author examines the models for ensuring information sovereignty in China and Russia, and proposes recommendations for developing an optimal hybrid model of information sovereignty for the Russian Federation.*

Key words: *information sovereignty; People's Republic of China; Russian Federation; comparative legal analysis; critical information infrastructure; legal liability.*

Введение. В эпоху глобальной цифровизации информационный суверенитет стал базовым элементом государственного суверенитета и условием обеспечения национальной безопасности. Способность государства контролировать свое информационное пространство сегодня подвергается беспрецедентным вызовам. Эта проблема резко обострилась в условиях масштабного санкционного давления и проведения специальной военной операции (СВО). Эти факторы обнажили уязвимость информационного пространства и критической информационной инфраструктуры перед внешними воздействиями.

Среди источников угроз национальной безопасности в информационной сфере и вызовами для государственного суверенитета, ключевое значение имеют:

трансграничные корпорации, которые фактически монополизировали каналы распространения информации. Они самостоятельно опреде-

ляют правила модерации контента. Примером жесткой цензуры и ограничения распространения отечественного контента является политика видеохостинга YouTube (принадлежащего корпорации Google LLC) [1]. Аналогичную политику проводят и другие западные экосистемы. Так корпорация Meta Platforms Inc. (признана в РФ экстремистской организацией) ввела беспрецедентные послабления в правилах модерации своих соцсетей Facebook и Instagram [2]. А Twitter (современное название платформы «X») системно присваивал государственным российским аккаунтам и профилям журналистов ограничительные маркеры [3]. Одновременно сохраняя доступ российской аудитории к «информации экстремистского характера, детская порнография, суицидальный контент, информация о продаже и пропаганде наркотиков» [4].

Подобные скоординированные действия трансграничных корпораций доказывают, что архитектура рекомендательных алгоритмов и правил модерации западных ИТ-компаний используется не как нейтральный технологический инструмент, а как цифровое воздействие на российскую и международную аудиторию, формируя однобокую повестку и ограничивая право на доступ к альтернативной точке зрения. Это превращает регулирование деятельности таких корпораций в важнейшую задачу обеспечения суверенитета государства;

международные акторы – к ним относятся иностранные государственные институты и хакерские группировки используют цифровое пространство как инструмент ведения гибридной войны. Их деструктивное воздействие на информационное пространство РФ проявляется в двух направлениях:

кибератаки и цифровой саботаж. На протяжении 2022–2025 гг. в России ежегодно фиксируется от 31 до 38 тыс. подтвержденных сложных инцидентах ИБ. [5], [6],[7];

финансирование и разработка инструментов прорыва цифровых границ. Примером прямого вмешательства в информационный суверенитет РФ является деятельность американского правительственного «Фонда открытых технологий» [8];

внутренние социальные группы за счет целенаправленного информационно-психологического воздействия на отдельные группы российского общества через:

распространение фейков и манипуляций в отношении молодежи [9]. Более того, фиксируются опасные прецеденты институционального вовлечения несовершеннолетних в противоправную деятельность, например, [10], [11];

воздействие на лидеров общественного мнения и представителей творческой интеллигенции посредством получения ими от международных акторов грантового и рекламного финансирования для формирования внутри страны пула лидеров мнений (реестр иностранных агентов [12]).

В этих реалиях возникает необходимость глубокого сравнительного анализа подходов к регулированию информационного пространства в России и за рубежом (на примере Китая), что определяет тему исследования, результаты которого представлены в настоящей статье.

Цель настоящей работы заключается в проведении комплексного сравнительно-правового анализа моделей законодательного регулирования информационного пространства в РФ и КНР для выявления институциональных уязвимостей отечественной правовой системы и выработки рекомендаций по формированию оптимальной гибридной модели обеспечения информационного суверенитета России.

Материалы и методы. Для достижения поставленной цели и обеспечения достоверности выводов использован репрезентативный массив нормативно-правовых, аналитических и эмпирических материалов. В процессе работы над статьей использовались общенаучные и специальные методы исследования, среди которых: сравнительно-правовой метод, системно-структурный анализ, дискурс-анализ, институциональный анализ.

Результаты и обсуждения. В мировой практике сформировались различные концептуальные подходы к делимитации и защите национального цифрового пространства.

Китайская модель регулирования характеризуется тотальным государственным контролем над потоками входящего и исходящего трафика. В КНР создана суверенная цифровая экосистема, состоящая из национальных аналогов глобальных платформ (Baidu, WeChat, Weibo). Ч. Шици провел ретроспективный анализ развития социальных медиа в Китае, в результате которого автор приходит к выводу: «китайская цифровая среда формирует не классическую публичную сферу, а ее гибридный аналог, который можно охарактеризовать как «управляемую», или «государственно-корпоративную» публичную сферу. Автономия от государства здесь является фикцией; платформы выступают в роли посредников, реализующих государственную политику в области информации» [13]. Ч. Шици выделил четыре концепции государственного контроля «Великий китайский файрвол», «Золотой щит» (микроуровень, «Гармонизация контента» (микроуровень), «Управление общественным мнением» [13].

Фундаментальным нормативным правовым

актом Китая, регулирующим цифровую среду, защиту данных и национальный суверенитет киберпространства (网络空间主权) является Закон КНР «О кибербезопасности» (中华人民共和国网络安全法), принятый в 2016 году и вступивший в силу 1 июня 2017 года [14]. Закон заложил основу для жесткого государственного контроля над ИТ-инфраструктурой. Поправки 2025 г. значительно ужесточили ответственность и расширили сферу действия этого закона на искусственный интеллект (ИИ), а также прямо закрепили норму о том, что обеспечение кибербезопасности осуществляется под строгим руководством Коммунистической партии Китая (КПК).

Закон определяет ключевые понятия:

сеть относится к системе, состоящей из компьютеров или других информационных терминалов и связанного с ними оборудования, которое собирает, хранит, передает, обменивается и обрабатывает информацию в соответствии с определенными правилами и процедурами;

кибербезопасность (сетевая безопасность) относится к способности предотвращать атаки, вторжение, помехи, разрушение и незаконное использование сети, а также несчастные случаи путем принятия необходимых мер для поддержания сети в стабильном и надежном рабочем состоянии и обеспечения целостности, конфиденциальности и доступности сетевых данных [14].

Главный постулат закона заключается в том, что юрисдикция Китая полностью распространяется на его цифровые границы. Государство имеет право регулировать, контролировать и блокировать любой контент или ИТ-процессы внутри страны. Закон официально включил генеративные модели и технологии ИИ в сферу регулирования информационной безопасности, требуя от разработчиков исключать генерацию деструктивного или подрывающего национальную безопасность контента. Примечательно, что российская генеративная модель Алиса AI на вопрос: «Крым чей?» отвечает «политически корректно»: «…Таким образом, вопрос о принадлежности Крыма остаётся спорным и зависит от политической позиции и точки зрения».

Возвращаясь к обзору Закон КНР, следует отметить, что нормами предусмотрена группировка субъектов ИТ-рынка с определением для каждой категории соответствующих обязанностей. Так, сетевые операторы (网络运营者) обязаны регистрироваться под реальными именами (实名制), провайдеры и платформы обязаны требовать от пользователей верификацию по паспорту или номеру телефона при регистрации. При этом анонимный доступ к созданию контента запрещен. Операторы должны сохранять системные логи сетевой активности не менее 6 месяцев и оказывать техническую помощь спецслужбам при расследовании преступлений.

Законом КНР в отдельном разделе главы 3 предусмотрены механизмы защиты ключевой информационной инфраструктуры. Персональные данные граждан КНР и важные государственные данные должны физически храниться на территории Китая. Вывод данных за рубеж требует строгой государственной проверки безопасности (Security Assessment). Любое телекоммуникационное и защитное оборудование перед закупкой для нужд критической информационной инфраструктуры должно проходить государственную сертификацию на отсутствие уязвимостей и «закладок».

Законом запрещен сбор персональных данных без явного информирования и согласия граждан. Сетевые операторы обязаны немедленно прекращать передачу незаконной информации, удалять её, сохранять записи о нарушениях и сообщать в контролирующие органы.

Глава VI «Юридическая ответственность» (法律责任) Закона КНР «О кибербезопасности» определяет систему наказаний за нарушения в сетевом пространстве. С учетом масштабного пакета поправок, вступивших в силу 1 января 2026 года, эта глава трансформировалась в один из самых жестких механизмов комплаенса в мире за счет кратного увеличения цены нарушений для бизнеса и введение сквозной персональной ответственности руководителей (таблица).

В РФ аналогичного по названию нормативного правового акта нет. Однако ряд аналогичных норм законодательно закреплены. Так, Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [15] является аналогом китайской Главы 3. Он регулирует защиту стратегических сетей (транспорт, банки, энергетика), обязывает передавать данные об инцидентах в государственные органы и требует постепенного отказа от иностранного оборудования. Несмотря на то, что перечень сфер, объекты которых отнесены к критической инфраструктуре в законодательных актах практически одинаков, усматривается отличие в привязке данных таких объектов к угрозам национальной безопасности, экономике и национальным интересам. Таким образом, по нашему мнению, происходит гармонизация стратегических документов различного срока планирования и норм закона.

Статья 7 возлагает обязанность по определению категории значимости (всего их три – с первой по третьей) на самого субъекта критической инфраструктуры согласно Правил категорирования объектов критической информационной инфраструктуры Российской Федерации [16].

Статья 31 Закона КНР устанавливает обязанность по такому определению за государственным органом, что сокращает возможность вариации при определении категорий, но вместе с тем сокращает объем работ государственного органа по группировки анализируемых объектов. Сопоставление требований по информированию и об атаках и инцидентах позволяет выявить различие в подходах. Если в РФ акцент сделан на реакцию на инциденты и информирование ФСБ РФ о таких инцидентах (ст. 9 ФЗ-187), то в Законе КНР (ст. 34) предусматривается обязанность операторов реализовывать превентивные меры защиты, такие как планирование реагирования и проведение учений.

В РФ и КНР предусмотрена централизованная система сбора и анализа информации об угрозах объектам критической инфраструктуры. Однако в РФ (ст. 5, 11) оператор является активным участником системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. В Законе КНР роль оператор ограничивается сбором и передачей информацией об обнаружении уязвимостей, но система управления представлена государственными органами (ст. 39).

Контроль в области безопасности объектов критической инфраструктуры в РФ организуется посредством плановых и внеплановых проверок Федеральной службы по техническому и экспортному контролю (статья 13 ФЗ-187). В КНР проверка безопасности находится в зоне ответственности операторов, которые должны проводить ежегодный внутренний аудит безопасности (ст. 34) и минимум один раз в год проводить комплексную оценку рисков безопасности сетей самостоятельно либо с привлечением сертифицированных агентств и отправлять отчеты властям (ст. 38).

В Российской Федерации ответственности и наказание за неисполнение требований закона норм определена отсылочной нормой на КоАП РФ и УК РФ (таблица).

Регулирование в сфере обеспечения информационного суверенитета включает Закон Китайской Народной Республики «О безопасности данных» (中华人民共和国数据安全法) (далее - DSL КНР) [17]. Если Закон КНР о кибербезопасности защищает инфраструктуру и сети, то этот закон защищает саму информацию как стратегический национальный ресурс. Закон юридически закрепляет, что любые данные, сгенерированные на территории Китая, подлежат суверенному контролю государства. Государство декларирует право регулировать их оборот, обогащение, хранение и уничтожение в целях национальной безопасности. Закон устанавливает классификацию данных и иерархическую систему защиты для классификации и защиты данных на основе важности данных для экономического и социального развития и степени ущерба, причиненного национальной безопасности, общественным интересам или законным правам и интересам отдельных лиц и организаций:

обычные данные, к ним относятся стандартная коммерческая и операционная информация;

важные данные (重要数据) – это сведения, утечка которых может навредить экономике или региональной безопасности.

ключевые государственные данные (核心数据) – затрагивающие национальную безопасность, жизненно важные интересы национальной экономики, важнейшие аспекты жизнеобеспечения населения, а также существенные общественные интересы. За нарушение правил работы данным и предусмотрены максимальные штрафы (до 10 млн юаней) и закрытие бизнеса [17].

В Российской Федерации категорированию подлежат не массивы данных как обособленный ресурс, а информационные системы, в которых они циркулируют. Законодательство закрепляет многоуровневую шкалу: в сфере государственных информационных систем (ГИС), требования к защите которых установлены ст. 16 ФЗ № 149-ФЗ [18] (включая нормы о переходе на единую платформу «ГосТех»), выделяются 1, 2 и 3 классы защищенности на основании нормативных актов ФСТЭК России (Приказ № 17) [19]. Для персональных данных предусмотрены четыре уровня защищенности – от УЗ-1 до УЗ-4 (в развитии ст. 19 ФЗ № 152-ФЗ [20] согласно Постановлению Правительства РФ № 1119 [21]). Критерием деления, как и в ст. 21 DSL КНР, выступает масштаб возможных негативных последствий для безопасности государства. Однако если китайский DSL категорирует саму информацию, российский законодатель в ст. 16 ФЗ № 149-ФЗ и актах регуляторов задействует инфраструктурный фильтр, классифицируя среду её обработки.

Следует отметить экстерриториальный суверенитет, предусмотренный Законом. Статья 2 прямо указывает: если организация или физическое лицо за пределами Китая осуществляет обработку данных, которая «наносит вред национальной безопасности или общественным интересам КНР», Китай имеет право привлечь их к юридической ответственности (включая экономические санкции и блокировки) [17]. Прямого аналога данной нормы в российском законодательстве нет, ч. 3 ст. 12 УК РФ, закрепляет реальный принцип экстерриториальности, так, иностранные граждане, совершившие киберпреступление вне пределов РФ (например, посягательство на российские государственные данные по ст. 272–274.1 УК РФ), подлежат ответственности, если

преступление направлено против интересов Российской Федерации.

Закон КНР «О защите персональной информации» (个人信息保护法) (далее - PIPL) [22], вступил в силу 1 ноября 2021 г. и является третьим «столпом законодательства Китая в области обеспечения информационного суверенитета. Аналогом PIPL является Федеральной закон РФ № 152-ФЗ «О персональных данных», анализ законодательных актов позволяет сделать вывод от высокой степени конвергенции правовых систем.

Законом исключен любой скрытый, принудительный или вводящий в заблуждение сбор данных. Прямым аналогом данной превентивной нормы в российском законодательстве выступает часть 1 статьи 9 ФЗ № 152-ФЗ, устанавливающая сквозной критерий юридической силы согласия на обработку данных. Согласно отечественной норме, такое согласие должно быть конкретным, предметным, информированным, сознательным и однозначным. Персональная информация должна удаляться или анонимизироваться сразу после достижения целей обработки. Прямым аналогом данного принципа в российском правовом поле выступает часть 7 статьи 5 ФЗ № 152-ФЗ, императивно требующая уничтожения обрабатываемых персональных данных либо их обезличивания по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Персональные данные разделена на обычные (имя, базовая контактная информация, пол, возраст) и чувствительные, данные, утечка которых может нанести вред человеческому достоинству, безопасности или имуществу. (биометрия – лицо и отпечатки, религиозные убеждения, медицинские карты, финансовые счета, трекинг геолокации в реальном времени, а также любые данные детей до 14 лет). Для обработки чувствительных данных компания обязана получить отдельное целенаправленное согласие пользователя. Пакетированные согласия («принимаю всё сразу») в КНР запрещены. В российском законодательстве аналогом данной дифференциации выступает разделение данных на общие, специальные (статья 10 ФЗ № 152-ФЗ) и биометрические (статья 11 ФЗ № 152-ФЗ). Правовой режим обработки специальных и биометрических данных в РФ полностью симметричен китайскому (ч. 4 ст. 9 ФЗ № 152-ФЗ) для них требуется исключительно письменное (или равнозначное ему электронное с усиленной подписью) целенаправленное согласие субъекта. Требование конкретности и предметности согласия в отечественном праве де-юре исключает легитимность «пакетированных» согласий, обязывая операторов предоставлять пользователю возможность выбора отдельных целей обработки, что демонстрирует концептуальное единство защитных механизмов РФ и КНР.

Ст. 24 запрещает платформам (такси, бронирование отелей, маркетплейсы) использовать автоматизированное профилирование для установления дискриминационных (более высоких) цен транзакций и других условий транзакций. Если реклама или контент формируются алгоритмом на базе персональных данных, пользователю обязаны предоставить кнопку «выключить персонализацию» или предложить альтернативный вариант, не привязанный к его цифровому профилю.

Закон имеет глобальный охват (ст. 3). Он применяется к иностранным компаниям за пределами Китая, если они предоставляют товары или услуги физлицам на территории КНР и / или анализируют и оценивают поведение граждан внутри Китая (например, через аналитические куки или трекеры приложений). Такие зарубежные компании обязаны учредить в Китае специальное юридическое лицо или назначить местного представителя, который будет нести административную ответственность перед Администрацией киберпространства Китая (CAC) и уголовную ответственность в рамках судебной системы КНР.

Оба акта выходят за рамки исключительно технического контроля, смещая фокус на защиту прав субъекта данных. Так, экстерриториальный контур статьи 3 PIPL концептуально совпадает с частью 1.1 статьи 1 ФЗ № 152-ФЗ, а обязанность открытия физических представительстве для зарубежных ИТ-платформ (статья 53 PIPL) в российском правовом поле дублируется, но в другом акте в Федеральном законе от 01.07.2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети „Интернет“ на территории Российской Федерации». Главное различие кроется в ответственности и механизме экономических санкций.

Следует отметить, что формирование регуляторного контура информационного суверенитета КНР продолжается. Как отмечает С. Бо в апреле 2026 года Администрацией киберпространства Китая (CAC) выпустила два противоположных по духу документа. Первый документ предлагает послабления для малого бизнеса, а второй запускает жесткие межведомственные проверки в шести ключевых индустриях (App/SDK, реклама, образование, транспорт, здравоохранение, финансы). Автор отмечает, что это не противоречие в политике, а переход китайского комплаенс-регулирования к модели многоуровневого управления [23].

Нами проведён анализ норм законодательства в области обеспечения информационного суверенитета в КНР и РФ, за нарушение которых предусматривается возникновение юридической ответственности в КНР и РФ (таблица).

Таблица - Сравнительный анализ юридической ответственности за нарушение норм

Нарушение	Санкции для юрлиц (КНР)	Персональные санкции для топ-менеджеров (КНР)	Аналогичные санкции и статьи в законодательстве РФ
1. Нарушение правил КИИ (закупки без проверки, трансграничный вывод данных)	Фиксированный штраф от 100 тыс. до 10 млн юаней; приостановка работы сайтов/ПО; отзыв лицензий	Личный штраф до 1 млн юаней; пожизненный запрет занимать руководящие должности в ИТ-секторе	Ст. 13.12.1 КоАП РФ – штраф до 50 тыс. руб. для физ. лиц, для юр. лиц от 50 тыс. до 100 тыс. руб.; за нарушение требований безопасности объектов КИИ (ч. 1) от 10 тыс. до 50 тыс. руб/ и от 100 тыс. до 500 тыс. руб. за нарушение порядка информирования об инцидентах соответственно
			Ст. 274.1 УК РФ. В случае наступления вредных последствий для должностного лица до 10 лет лишения свободы
2. Игнорирование анонимности (оказание услуг без проверки реального имени/паспорта)	Штраф от 50 тыс. до 500 тыс. юаней; приостановка операций; полное закрытие веб-ресурса.	Личный штраф от 10 тыс. до 100 тыс. юаней	Ст. 13.31 КоАП РФ. Административный штраф для юр. лиц от 800 тыс. до 1 млн. руб. (ч. 2) за неисполнение бланкетного требования ст. 10.1 ФЗ № 149-ФЗ об обязательной верификации пользователей (включая идентификацию по номеру телефона)
			Ст. 13.29 КоАП РФ. Штраф для операторов связи и дилеров за несоблюдение порядка верификации абонентов (включая продажи без паспорта и превышение лимитов на сим-карты) от 300 тыс. до 500 тыс. руб. (для юр. лиц), а при повторных грубых нарушениях или отсутствии данных в ЕСИА – от 1 млн до 2 млн руб.
3. Пропуск вредоносного контента (распространение запрещенной информации, деструктивного контента ИИ)	Крупные штрафы; конфискация незаконно полученного дохода; блокировка платформ	Личные штрафы; административный арест за содействие правонарушению	Ст. 13.41 КоАП РФ: Оборотные штрафы для владельцев сайта или информационного ресурса в сети "Интернет" в размере от 1/20 до 1/5 совокупного размера годовой вы-

			ручки (за повторное нарушение)
			Персональная ответственность высших должностных лиц в виде ареста предусмотрена в случае умышленного неисполнения судебного решения об удалении контента (ч. 2 ст. 315 УК РФ) , предусматривающую персональный арест до 6 месяцев или лишение свободы до 2 лет
4. Незаконный оборот данных и утечки (несоблюдение локализации, компрометация персональных данных)	Фиксированные штрафы до 10–50 млн юаней (по «О защите персональной информации» / «О безопасности данных») или оборотные до 5% от годовой выручки; ликвидация бизнеса	Личные штрафы до 1 млн юаней; уголовное преследование	Ст. 13.11 КоАП РФ (ч. 12–14). Первичные фиксированные штрафы за утечки персональных данных дифференцированы: от 3 до 5 млн руб. (за компрометацию данных от 1 тыс. до 10 тыс. субъектов) до 10–15 млн руб. (если затронуты более 100 тыс. субъектов или более 1 млн уникальных идентификаторов)
			При повторной утечке – оборотный штраф от 1% до 3% годовой выручки (но в границах от 20 млн. до 500 млн. руб.)

По нашему мнению, если китайский законодатель использует фиксированные штрафы до 10 млн юаней в качестве универсальной превентивной меры, то российский правовой подход к 2026 году пришел к гибридной схеме: сочетанию жестких фиксированных порогов (до 15–20 млн рублей за первичные инциденты с биометрией) и гигантских оборотных штрафов с нижним пределом в 20 млн и потолком в полмиллиарда рублей за повторные утечки.

Заключение. Проведенный анализ показывает высокую степень сближения норм законодательства РФ и КНР по государственному контролю цифрового пространства. Однако, выявленные различия позволяют применить успешный китайский опыт в российском законодательстве. В частности, дополнение Федерального закона № 149-ФЗ классификацией массивов данных (по аналогии с DSL КНР), позволит защищать стратегическую информацию независимо от того, в какой именно (государственной или частной) информационной системе она циркулирует. Также целесообразно закрепить в ФЗ № 149-ФЗ прямую норму об экстерриториальном действии российского информационного законодательства (по аналогии со ст. 2 DSL КНР) в отношении любых иностранных лиц, чьи действия по обработке данных наносят вред национальной безопасности или общественным интересам РФ. Дополнить КоАП РФ нормами о персональной ответственности топ-менеджмента ИТ-компаний персональными дисквалифицирующими санкциями, вплоть до пожизненного запрета на занятие руководящих должностей в ИТ-отрасли за грубые системные нарушения

Дополнить Федеральный закон № 187-ФЗ обязанностью субъектов критической инфраструктуры проводить ежегодный обязательный внутренний аудит и комплексную оценку рисков с предоставлением отчетов регуляторам (ФСТЭК, ФСБ), а также закрепить нормативную обязанность по регулярному проведению практических киберучений. Законодательно закрепить требования к разработчикам генеративного искусственного интеллекта и больших языковых моделей (LLM) по превентивному исключению гене-

рации контента, подрывающего конституционный строй и национальную безопасность РФ.

Список литературы:

[1] YouTube заблокировал уже более 80 российских каналов в этом году / Интерфакс : информационное агентство. – 2024. – 10 июля. – URL: https://www.interfax.ru/russia/970173 (дата обращения: 12.07.2026).

[2] Meta продлила разрешение на призывы к убийству российских военных до конца апреля / Коммерсантъ : газета. – 2022. – 11 апреля. – URL: https://www.kommersant.ru/doc/5304694 (дата обращения: 12.07.2026).

[3] В России заблокировали Twitter / 74.ру : сетевое издание. – 2022. – 5 марта. – URL: https://74.ru/text/world/2022/03/05/70488602/ (дата обращения: 12.07.2026).

[4] Роскомнадзор просит Twitter разъяснить причины блокировки нескольких российских аккаунтов / Официальный сайт Роскомнадзора. – 2019. – 16 декабря. – URL: https://old.rkn.gov.ru/press/publications/news71076.htm (дата обращения: 12.07.2026).

[5] Кибератаки на российские компании в 2024 году / ГК «Солар» : Центр исследования киберугроз : официальный сайт. – 2025. – URL: https://rt-solar.ru/analytics/reports/5320/ (дата обращения: 12.07.2026).

[6] За два года доля атак с вредоносным ПО на российскую промышленность выросла с 56 % до 83 % / SecPost : сетевое издание в сфере ИБ. – 2026. – 19 мая. – URL: https://secpost.ru/za-dva-goda-dolya-atak-s-vredonosnym-po-na-rossijskuyu-promyshlennost-vyrosla-s-56-do-83 (дата обращения: 12.07.2026).

[7] Кибервойна России и Украины / TAdviser : государственно-коммерческий портал. – 2025. – 5 ноября. – URL: https://clck.ru/3UhkQF (дата обращения: 12.07.2026).

[8] Pearson, J. US calls on Big Tech to help evade online censors in Russia, Iran / J. Pearson // Reuters : global news agency. – 2024. – September 5. – URL: reuters.com (дата обращения: 12.07.2026).

[9] Лига безопасного интернета выявила более 13 млн фейков о России с начала СВО / ТАСС : информационное агентство. – 2024. – 25 января. – URL: tass.ru (дата обращения: 12.07.2026).

[10] В Первоуральске подростка обвинили в диверсии на железной дороге / РИА Новости : информационное агентство. – 2026. – 9 июля. – URL: https://ria.ru/20260709/sk-2103718528.html (дата обращения: 12.07.2026).

[11] Подростка, который поджёг подстанцию в Подмосковье, обвинили в теракте / РИА Новости : информационное агентство. – 2026. – 2 июля. – URL: ria.ru (дата обращения: 12.07.2026).

[12] Реестр иностранных агентов / Министерство юстиции Российской Федерации : официальный сайт. – 2026. – URL: minjust.gov.ru (дата обращения: 12.07.2026).

[13] Шици, Ч. История развития социальных медиа в Китае / Ч. Шици // Мир науки, культуры, образования. – 2025. – № 6 (115). – С. 543–546.

[14] 中华人民共和国网络安全法 (Закон Китайской Народной Республики «О кибербезопасности») / Официальный сайт Управления киберпространства КНР (САС). – URL: https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm (дата обращения: 10.07.2026).

[15] Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 07.04.2025) «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=502634&dst=100001%2C-1&date=13.07.2026&demo=2 (дата обращения: 09.07.2026).

[16] Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 07.11.2025) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». – URL: http://government.ru/docs/all/115353/2 (дата обращения: 10.07.2026).

[17] 中华人民共和国数据安全法 (Закон Китайской Народной Республики «О безопасности данных») / Официальный сайт Управления киберпространства КНР (САС). – URL: https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm (дата обращения: 09.07.2026).

[18] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 26.06.2026) «Об информации, информационных технологиях и о защите информации». – URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=538088&dst=100001%2C-1&date=12.07.2026&demo=2 (дата обращения: 12.07.2026).

[19] Федеральная служба по техническому и экспортному контролю. Приказ от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (ред. от 28.08.2024) / Официальный сайт ФСТЭК России. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 12.07.2026).

[20] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных». – URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/ (дата обращения: 12.07.2026).

[21] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». – URL: https://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100025 (дата обращения: 12.07.2026).

[22] 个人信息保护法 (Закон Китайской Народной Республики «О защите персональной информации») / Официальный сайт Управления киберпространства КНР (CAC). – URL: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm (дата обращения: 09.07.2026).

[23] Сунь, Бо. Натяжение и ослабление: регуляторная система защиты персональных данных в Китае вступает в эпоху многоуровневого управления = 张一弛：中国个人信息保护进入监管分层时代 / Сунь Бо. – Текст : электронный // 君合法律评论 : [официальный сайт юридической фирмы JunHe]. – 2026. – 10 апреля. – URL: junhe.com (дата обращения: 12.07.2026).

References:

[1] YouTube has already blocked more than 80 Russian channels this year/Interfax: News Agency. – 2024. - July 10. - URL: https://www.interfax.ru/russia/970173 (access date: 12.07.2026).

[2] Meta extended permission to call for the murder of the Russian military until the end of April/Kommersant: newspaper. – 2022. - April 11. - URL: https://www.kommersant.ru/doc/5304694 (access date: 12.07.2026).

[3] Twitter/ 74.py blocked in Russia: online edition. – 2022. - March 5. - URL: https://74.ru/text/world/2022/03/05/70488602/ (access date: 12.07.2026).

[4] Roskomnadzor asks Twitter to clarify the reasons for blocking several Russian accounts/ Official website of Roskomnadzor. – 2019. - December 16. - URL: https://old.rkn.gov.ru/press/publications/news71076.htm (access date: 12.07.2026).

[5] Cyberattacks on Russian companies in 2024/Solar Group of Companies: Cyber Threat Research Center: official website. – 2025. - URL: https://rt-solar.ru/analytics/reports/5320/ (access date: 12.07.2026).

[6] In two years, the share of malware attacks on the Russian industry has grown from 56% to 83 %/SecPost: online information security publication. – 2026. - May 19. – URL: https://secpost.ru/za-dva-goda-dolya-atak-s-vredonosnym-po-na-rossijskuyu-promyshlennost-vyrosla-s-56-do-83 (дата обращения: 12.07.2026).

[7] Cyberwar of Russia and Ukraine/TAdviser: public-commercial portal. – 2025. - November 5. - URL: https://clck.ru/3UhkQF (access date: 12.07.2026).

[8] Pearson, J. US calls on Big Tech to help evade online censors in Russia, Iran / J. Pearson // Reuters : global news agency. – 2024. – September 5. - URL: reuters.com (access date: 12.07.2026).

[9] The Safe Internet League has identified more than 13 million fakes about Russia since the beginning of the SVO/TASS: news agency. – 2024. - January 25. - URL: tass.ru (access date: 12.07.2026).

[10] In Pervouralsk, a teenager was accused of sabotage on the railway/RIA Novosti: news agency. – 2026. - July 9. - URL: https://ria.ru/20260709/sk-2103718528.html (access date: 12.07.2026).

[11] A teenager who set fire to a substation in the suburbs was accused of a terrorist attack/RIA Novosti: news agency. – 2026. - July 2. - URL: ria.ru (access date: 12.07.2026).

[12] Register of foreign agents/Ministry of Justice of the Russian Federation: official website. – 2026. - URL: minjust.gov.ru (access date: 12.07.2026).

[13] Shitsi, C. History of the development of social media in China/C. Shitsi // World of science, culture, education. – 2025. – № 6 (115). - S. 543-546.

[14] 中华人民共和国网络安全法 (Cybersecurity Law of the People's Republic of China)/Official Website of the Cyberspace Administration of the PRC (CAC). - URL: https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm (access date: 10.07.2026).

[15] Federal Law No. 26.07.2017 of 187-FZ (as amended by 07.04.2025) "On the Security of the Critical Information Infrastructure of the Russian Federation." - URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=502634&dst=100001%2C-1&date=13.07.2026&demo=2 (access date: 09.07.2026).

[16] Decree of the Government of the Russian Federation of 08.02.2018 No. 127 (as amended by 07.11.2025) "On Approval of the Rules for Categorizing Critical Information Infrastructure Facilities of the Russian Federation, as well as a List of Indicators of the Significance of Critical Information Infrastructure Facilities of the Russian Federation and Their Values." - URL: http://government.ru/docs/all/115353/2 (access date: 10.07.2026).

[17] 中华人民共和国数据安全法 (Data Security Law of the People's Republic of China)/Official website of the PRC Cyberspace Administration (CAC). - URL: https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm (access date: 09.07.2026).

[18] Federal Law No. 149-FZ of 27.07.2006 (as amended by 26.06.2026) "On Information, Information Technologies and Information Protection." - URL: https://login.consultant.ru/link/?req=doc&base=LAW&n=538088&dst=100001%

2C-1&date=12.07.2026&demo=2 (access date: 12.07.2026).

[19] Federal Service for Technical and Export Control. Order No. 17 dated 11.02.2013 "On Approval of Requirements for Protection of Non-State Secret Information Contained in State Information Systems" (as amended by 28.08.2024) /Official website of the FSTEC of Russia. – URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 12.07.2026).

[20] Federal Law No. 27.07.2006 dated 152-FZ (as amended 24.06.2025) "On Personal Data." - URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ca9e5658710519f09ab2fdb8196fcb3eb024a051/ (access date: 12.07.2026).

[21] Decree of the Government of the Russian Federation of 01.11.2012 No. 1119 "On approval of requirements for the protection of personal data during their processing in personal data information systems." - URL: https://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100025 (access date: 12.07.2026).

[22] 个人信息保护法 (Law of the People's Republic of China "On the Protection of Personal Information")/Official website of the Cyberspace Administration of the PRC (CAC). - URL: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm (access date: 09.07.2026).

[23] Sun, Bo. Tightening and loosening: China's regulatory system for personal data protection is entering an era of multilevel governance = 张一弛: 中国个人信息保护进入监管分层时代/Sun Bo. - Text: electronic // 君合法律评论: [official website of JunHe Law Firm]. – 2026. - April 10. - URL: junhe.com (access date: 12.07.2026).

