DOI: 10.24412/2075-7913-2026-2(102)-106-111

УДК 343.9:343.3/.8

Петров П. К., Денисович В. В.

НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *Политика кибербезопасности Китая опирается на сложную систему законодательных актов, подзаконных документов, институциональных структур и технологических решений. Вместе они формируют механизм, направленный на выполнение задач, определённых в стратегических документах. Центральным элементом этой системы являются базовые законы, которые устанавливают правовые рамки для регулирования информационного пространства, защиты данных и инфраструктуры. На их базе разрабатываются подзаконные акты и технические регламенты, конкретизирующие общие положения в различных областях. Исполнение законодательства осуществляется государственными органами, наделёнными соответствующими полномочиями в сфере кибербезопасности.*

Ключевые слова: *кибербезопасность, правовое регулирование информационной безопасности, цифровое право цифровая преступность, цифровая дипломатия*

Финансирование: *Работа выполнена за счет гранта, предоставленного Академией наук Республики Татарстан образовательным организациям высшего образования, научным и иным организациям на поддержку планов развития кадрового потенциала в части стимулирования их научных и научно-педагогических работников к защите докторских диссертаций и выполнению научно-исследовательских работ.*

Для цитирования: Петров П. К., Денисович В. В. Нормативно-правовое регулирование в сфере информационной безопасности // Проблемы права. 2026. № 2 (102). С. 106–111. DOI: 10.24412/2075-7913-2026-2(102)-106-111

Petrov P. K., Denisovich V. V.

LEGAL REGULATION IN THE FIELD OF INFORMATION SECURITY

Abstract. *China's cybersecurity policy relies on a complex system of statutes, bylaws, institutional structures and technological solutions. Together, they form a mechanism aimed at fulfilling the tasks defined in the strategic documents. The central element of this system is the basic laws that establish the legal framework for regulating the information space, data protection and infrastructure. On their basis, by-laws and technical regulations are developed that specify general provisions in various fields. The implementation of legislation is carried out by state bodies endowed with appropriate powers in the field of cybersecurity.*

Keywords: *cybersecurity, legal regulation of information security, digital law digital crime, digital diplomacy*

For citation: Petrov P. K., Denisovich V. V. Legal Regulation in the Field of Information Security. *Problemy prava (Issues of Law)*. 2026. No. 2 (102). P. 106–111. DOI: 10.24412/2075-7913-2026-2(102)-106-111

Принятый в ноябре 2016 г. и вступивший в силу 1 июня 2017 г., Закон о кибербезопасности КНР стал первым комплексным нормативным актом в области регулирования киберпространства[1]. До его появления законодательство в этой сфере ограничивалось разрозненными подзаконными актами, которые касались защиты компьютерных систем и информационной инфраструктуры. Новый закон ознаменовал переход к системному подходу в управлении кибербезопасностью.

Структура закона включает семь глав, охватывающих основные аспекты: общие положения, меры по обеспечению кибербезопасности, безопасность сетевых операций (с особым разделом о критической информационной инфраструктуре), защиту данных в сети, мониторинг и реагирование на угрозы, а также вопросы ответственности за нарушения.

Основные понятия, закреплённые в законе, формируют основу для последующего регулирования. Операторами сети признаются собственники, администраторы сетей и провайдеры сетевых услуг. Сетевые данные определяются как любая информация, обрабатываемая в цифровом пространстве. Персональные данные включают сведения, позволяющие идентифицировать физическое лицо, такие как имя, дата рождения, биометрические данные и номер телефона.

Государство берёт на себя широкий круг обязанностей: разработка стратегии кибербезопасности, защита критической инфраструктуры, мониторинг угроз, международное сотрудничество, установление стандартов и защита прав граждан. Для выполнения этих задач создаётся специальный орган — Администрация кибербезопасности Китая (CAC), а также соответствующие подразделения в органах власти всех уровней.

Операторы сетей обязаны соблюдать законодательство, обеспечивать безопасность, идентифицировать пользователей, хранить данные, взаимодействовать с властями и оперативно реагировать на инциденты. Закон также запрещает использование сети для деятельности, направленной против государственной власти, социалистического строя, территориальной целостности, а также для пропаганды терроризма, экстремизма, насилия, порнографии и распространения дезинформации.

Особое внимание уделяется разделу о критической информационной инфраструктуре (далее — КИИ). Закон относит к КИИ ключевые отрасли, такие как информационно-коммуникационные услуги, энергетика, транспорт, водное хозяйство, финансы и государственные услуги. Нарушение работы этих секторов может представлять угрозу национальной безопасности или жизнеобеспечению населения [4]. Для операторов КИИ установлены дополнительные требования, включая обязательное хранение персональных данных на территории Китая и особую проверку используемых продуктов и услуг на предмет их влияния на государственную безопасность.

Глава о защите информации регулирует режим охраны персональных данных: обеспечение конфиденциальности, сбор только необходимой информации, обезличивание данных, удаление незаконно полученной информации и сотрудничество с властями. Закон также запрещает создание ресурсов для незаконной деятельности и распространение вредоносной информации.

Таким образом, Закон о кибербезопасности КНР выполняет роль комплексного закона в сфере кибербезопасности, вводя базовые понятия и принципы, устанавливая особый режим для стратегических секторов и регулируя ответственность операторов. Появление данного закона означало переход в КНР от разрозненных нормативных актов к единому большому закону в сфере кибербезопасности. Его значение выходит за рамки технического регулирования, закрепляя за государством право контролировать информационные потоки, а за бизнесом — обязанность обеспечивать этот контроль. Последующие законы, такие как акты 2021 г. о данных и персональной информации, будут развивать нормы, заложенные в этом документе.

В июне 2021 г. в Китае был принят Закон о безопасности данных, который вступил в силу 1 сентября того же г..[2] Этот нор-

[1] Закон Китайской Народной Республики о кибербезопасности: принят Постоянным комитетом Всекитайского собрания народных представителей 7 нояб. 2016 г.: вступ. в силу 1 июня 2017 г. // СПС «Консультант+» [Электронный ресурс] — URL: https://ru.nia.gov.cn/n21914/n21970/index.html (дата обращения: 22.04.2026).

[2] Закон Китайской Народной Республики о безопасности данных: принят Постоянным комитетом Всекитайского собрания народных представителей 10 июня 2021 г.: вступ. в силу 1 сент. 2021 г. // СПС «Консультант+» [Электронный ресурс] — URL: https://www.chinajusticeobserver.com/law/x/data-security-law-of-the-people-s-republic-of-china20210610/enchn (дата обращения: 22.04.2026).

мативный акт стал второй частью триады ключевых законов в области кибербезопасности.. Впервые в китайской правовой системе было дано универсальное определение данных как любых записей информации в электронной или иной форме. Это означает, что закон регулирует не только цифровые, но и аналоговые данные. Действие закона охватывает все аспекты обработки данных на территории КНР. В некоторых случаях он может применяться и за пределами страны, если зарубежные компании наносят ущерб государственной безопасности или интересам граждан Китая.

Основной принцип закона — это классификация данных и многоуровневая система их защиты в зависимости от значимости. Выделяются два ключевых типа данных: «государственные основные данные», которые касаются безопасности государства, экономики и публичных интересов, и «важные данные», перечень которых определяется на национальном, отраслевом и региональном уровнях. Для каждой категории данных установлены повышенные требования к защите и ужесточена ответственность за нарушения. Операторы обязаны внедрять системы управления безопасностью, отслеживать угрозы, сообщать о инцидентах и помогать госорганам в раскрытии преступлений [2]. Особое внимание уделяется ограничениям на трансграничную передачу данных. Экспорт важных данных возможен только после проверки их безопасности. Передача данных иностранным правоохранительным органам возможна только с разрешения китайских властей.

Таким образом, закон закрепляет суверенитет КНР над данными и создаёт правовую основу для контроля за всеми видами информации, обрабатываемой в стране.

В 2021 г. также был принят Закон о защите персональной информации (PIPL), который стал завершающим элементом законодательной системы в области кибербезопасности[1]. Этот закон дополнил существующие нормативные акты, такие как Закон о кибербезопасности и Закон о безопасности данных. Несмотря на внешнее сходство с европейским GDPR, PIPL имеет принципиальные отличия. Его основная цель — не защита частной жизни как основополагающего права, а обеспечение национальной безопасности и общественных интересов. Это проявляется в том, что закон не ограничивает сбор данных государственными органами, предоставляет регуляторам широкую свободу действий и позволяет контролировать обработку данных граждан Китая за пределами страны.

Одним из ключевых нововведений PIPL являются требования к передаче данных за границу. Операторы КИИ обязаны локализовать свои данные, проводить оценку безопасности перед передачей за рубеж и запрещать передачу информации иностранным правоохранительным органам без предварительного согласия властей КНР. При этом чувствительными данными признаются не только традиционные категории, такие как биометрия и медицинские сведения, но и геолокация, финансовые данные и информация о лицах младше 14 лет. Ответственность за нарушения, предусмотренные PIPL, приближена к европейским стандартам и может включать штрафы до 5 % от годового оборота компании. Однако механизмы правоприменения предоставляют регуляторам значительные полномочия для воздействия на бизнес.

Таким образом, PIPL закрепляет суверенитет Китая над персональными данными и одновременно создаёт инструменты для контроля над глобальными цифровыми платформами, работающими с китайскими пользователями.

Три закона, принятые в 2017–2021 гг. сформировали целостную систему регулирования информационного пространства КНР. Если Закон о кибербезопасности 2017 г. заложил базовые принципы и создал институциональную основу, то законы 2021 г. конкретизировали и ужесточили требования к двум ключевым объектам: данным как таковым и персональной информации граждан.

Китайская модель кибербезопасности делает основной упор на обеспечение национальной безопасности и суверенитета над информационными ресурсами [1]. Это выражается в трёх ключевых аспектах: во-первых, в строгих требованиях к хранению данных внутри страны и ограничениях на их передачу за границу; во-вторых, в широких полномочиях регуляторов и отсутствии значительных ограничений для

[1] Закон Китайской Народной Республики о защите персональной информации: принят Постоянным комитетом Всекитайского собрания народных представителей 20 авг. 2021 г.: вступ. в силу 1 нояб. 2021 г. // СПС «Консультант+» [Электронный ресурс] — URL: https://www.chinajusticeobserver.com/law/x/data-security-law-of-the-people-s-republic-of-china20210610/enchn (дата обращения: 22.04.2026).

государственных органов при сборе и анализе информации; в-третьих, в контроле деятельности иностранных компаний, работающих с китайскими данными.

В итоге эти законы формируют правовой механизм, позволяющий государству контролировать все виды данных на его территории. В этой системе кибербезопасность становится инструментом для реализации цифрового суверенитета, где защита информации и государственные интересы тесно переплетаются.

Однако сами по себе законы устанавливают лишь общие рамки. Их практическое применение требует конкретизации через подзаконные акты и технические стандарты. Эти документы превращают абстрактные нормы в чёткие требования для операторов, процедуры проверок и обязательные технические регламенты. Именно на этом уровне общие законодательные принципы превращаются в действующие механизмы контроля.

Многоуровневая схема защиты кибербезопасности (далее — MLPS) была введена в 2008 г. и обновлена в версии 2.0, которая вступила в силу в декабре 2019 г. Эта система классифицирует информационные системы по степени их важности и потенциальному ущербу в случае нарушения безопасности. В MLPS предусмотрено пять уровней чувствительности. Чем выше уровень, тем строже контроль со стороны Министерства общественной безопасности [4]. Ключевой порог установлен на третьем уровне, где самосертификация оператора заменяется обязательной правительственной проверкой. Этот уровень достигается, если нарушение системы может привести к серьёзным последствиям для прав граждан, общественного порядка или национальной безопасности.

С введением MLPS 2.0 значительно расширился перечень систем, подлежащих проверке. Теперь под действие схемы попадают все IT-системы, работающие в Китае. Операторы сетей, включая любые подключённые устройства и системы, обрабатывающие данные, обязаны классифицировать свои системы и применять соответствующие меры безопасности в зависимости от присвоенного уровня.

MLPS 2.0 поддерживается двумя дополнительными законами. Новый закон о криптографии запрещает разработку, продажу и использование криптографических систем, которые могут нанести ущерб государственной безопасности и общественным интересам. Непроверенные криптографические системы фактически становятся незаконными. Закон об иностранных инвестициях формально направлен на упрощение процедур, но на практике ограничивает права иностранных инвесторов, ставя их в равные условия с китайскими компаниями. Это, вместе с требованиями MLPS, создаёт дополнительные барьеры для иностранных инвесторов.

Особое внимание уделяется требованиям локализации данных. Если датацентр использует китайские программные сервисы, все данные, включая коммерческую тайну и финансовую информацию, могут быть изъяты государственными органами. MLPS 2.0 фактически предоставляет правительству неограниченный доступ ко всем данным в стране, независимо от того, где они хранятся или передаются. Это исключает возможность анонимного использования VPN, личной или зашифрованной переписки, а также конфиденциального хранения корпоративных данных.

1 сентября 2021 г. в Китае вступил в силу новый документ, уточняющий защиту КИИ и детализирующий нормы Закона о кибербезопасности 2017 г. Этот документ определяет порядок отнесения объектов к КИИ, обязанности операторов и меры ответственности за нарушения. КИИ включает критически важные сети в таких сферах, как телекоммуникации, энергетика, транспорт, ирригация, финансы, госуслуги, оборона и другие, и их нарушение может угрожать безопасности и экономике страны. Отраслевые регуляторы разрабатывают правила для защиты КИИ, которые регистрируются в Министерстве общественной безопасности. Операторы обязаны создавать службы безопасности, проверять сотрудников, оценивать уязвимости, информировать госорганы об инцидентах, выбирать надёжных поставщиков и проходить проверки, при этом меры защиты должны соответствовать уровню КИИ [5].

Контроль за соблюдением требований осуществляет Министерство общественной безопасности при участии Государственной канцелярии по делам интернет-информации. За нарушения предусмотрены значительные штрафы: до 1 миллиона юаней для операторов и до 100 тысяч для должностных лиц. Положение также вводит особый контроль за стратегически важными объектами, устанавливает персональную ответственность руководителей и механизмы реагирования на угрозы, формируя комплексную систему защиты КИИ,

направленную на обеспечение её устойчивости и безопасности.

Таким образом, правовое регулирование кибербезопасности в Китае представляет собой сложную многоуровневую систему, где основные законы задают общие принципы, а подзаконные акты и стандарты превращают эти принципы в практические механизмы. Ключевыми элементами этой системы являются Законы о кибербезопасности, о защите данных и о защите персональной информации. Закон о кибербезопасности 2017 г. ввёл основные понятия, создал институциональную основу и ввёл особый режим для критической информационной инфраструктуры. Законы 2021 г. уточнили и ужесточили требования к обработке данных и персональной информации, закрепив принципы суверенитета и локализации данных. На их основе сформировалась система подзаконного регулирования. Многоуровневая схема защиты разработала единую классификацию для всех IT-систем в Китае, связывая уровень потенциального ущерба с интенсивностью государственного контроля [6]. Особый режим для критической информационной инфраструктуры предусматривает персональную ответственность руководителей стратегических объектов, требует создания специализированных подразделений безопасности и устанавливает строгие требования к закупке оборудования и реагированию на инциденты. Законодательство о защите данных закрепляет принципы локализации и контроля за трансграничной передачей информации, создавая правовые препятствия для её неконтролируемого перемещения. В совокупности эти нормы формируют плотную нормативную среду, где технические стандарты и административные процедуры обеспечивают государственный контроль над цифровым пространством, а кибербезопасность становится инструментом реализации цифрового суверенитета.

Список литературы

1. Антонян Е. А. Китайский опыт борьбы с преступлениями в сфере информационных технологий // Вестник Университета имени О. Е. Кутафина. 2025. № 5 (129). — С. 150–158.
2. Горян Э. В. Безопасность персональных данных в КНР: тенденции совершенствования правового регулирования в финансово-банковском секторе // Административное и муниципальное право. 2021. № 5. — С. 15–27
3. Горян, Э. В. Закон о кибербезопасности Китайской Народной Республики как ключевой инструмент обеспечения информационной безопасности финансово-банковской системы // Административное и муниципальное право. — 2020. — № 3. — С. 47–55
4. Горян Э. В. Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики // Территория новых возможностей. 2021. № 1 — С. 115–122
5. Зверянская Л. П. Организационно-правовое обеспечение международной и национальной информационной безопасности: опыт Китайской Народной Республики // Труды Института государства и права РАН. 2017. № 5 (63). — С. 197–207
6. Кузнецова В. В. Практика цифровизации государственного управления в Китае // ФГУ. [Электронный ресурс] — URL: https://spa.msu.ru/wp-content/uploads/fgu_czifrovizacziya_pravit_kuzneczova.pdf (дата обращения: 11.02.2026)

References

1. Antonyan E. A. Chinese experience in combating crimes in the field of information technology//Bulletin of the O. E. Kutafin University. 2025. № 5 (129). — S. 150–158.
2. Goryan E. V. Security of personal data in the PRC: trends in improving legal regulation in the financial and banking sector//Administrative and municipal law. 2021. № 5. — S. 15–27
3. Goryan, E. V. Cybersecurity Law of the People's Republic of China as a key tool for ensuring information security of the financial and banking system//Administrative and municipal law. — 2020. — № 3. — S. 47–55
4. Goryan E. V. Regulatory framework for ensuring national security in cyberspace: the experience of the People's Republic of China//Territory of new opportunities. 2021. NO. 1 — P. 115–122
5. Zveryanskaya L. P. Organizational and legal support of international and national information security: the experience of the People's Republic of China//Proceedings of the Institute of State and Law of the Russian Academy of Sciences. 2017. № 5 (63). — S. 197–207
6. Kuznetsova V. V. Practice of digitalization of public administration in China//FSU. [Электронный ресурс] — URL: https://spa.msu.ru/wp-content/uploads/fgu_czifrovizacziya_pravit_kuzneczova.pdf (дата обращения: 11.02.2026)

Сведения об авторах

Петров Павел Константинович — кандидат юридических наук, доцент кафедры уголовного и уголовно-исполнительного права, криминологии НИУ «Южно-Уральский государственный университет», доцент. Председатель коллегии адвокатов НО «Коллегия Адвокатов г. Челябинска». E-mail: kollegiapetrov@mail.ru

Денисович Вероника Владимировна — старший научный сотрудник, кандидат юридических наук, доцент «Казанский инновационный университет имени В. Г. Тимирясова», г. Казань, Российская Федерация, доцент кафедры международных отношений, политологии и регионоведения института лингвистики и международных отношений «Южно-Уральский государственный университет» (НИУ). E-mail: LtybctyejV1984@yandex.ru

Information about the authors

Petrov Pavel Konstantinovich — Cand. Sci. (Law), Associate Professor of the Department of Criminal and Penal Enforcement Law, Criminology of the National Research University 'South Ural State University', Associate Professor. Chairman of the Bar Association 'Chelyabinsk Bar Association'. E-mail: kollegiapetrov@mail.ru

Denisovich Veronika Vladimirovna — Senior Researcher, Ph.D., Associate Professor, Kazan Innovation University named after V. G. Timiryasova, Kazan, Russian Federation, Associate Professor, Department of International Relations, Political Science and Regional Studies, Institute of Linguistics and International Relations, South Ural State University (NIU). E-mail: kollegiapetrov@mail.ru

Конфликт интересов отсутствует.
There is no conflict of interest.

Дата поступления статьи / Received: 22.01.2026

Дата рецензирования / Received: 23.02.2026

Дата принятия к опубликованию / Accepted: 25.03.2026