
КОДАНЕВА С.И.¹ ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ИНСТИТУЦИОНАЛЬНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ И В ЗАРУБЕЖНЫХ СТРАНАХ (Статья)

Аннотация. Кибербезопасность стала одной из наиболее важных областей политики в XXI в., выходящей за рамки традиционных национальных границ и переплетающейся с экономическими, социальными и геополитическими вопросами. Большинство стран мира принимает собственное правовое регулирование в данной сфере. Хотя реализуемые в национальном праве подходы и различаются в зависимости от правовых традиций и иных особенностей, однако нормативные акты в области информационной безопасности охватывают широкий спектр вопросов: от законов о защите данных и безопасности критически важной инфраструктуры до предотвращения киберпреступлений и защиты от информационно-психологического воздействия. В настоящей статье на основе анализа правовых подходов в различных странах мира формулируются общие тенденции развития права информационной безопасности.

Ключевые слова: кибербезопасность; защита данных; защита критической информационной инфраструктуры; информационная безопасность; киберсуверенитет; киберинциденты.

KODANEVA S.I. Legal regulation and institutional framework of information security in Russia and abroad. (Article)

Abstract. Cybersecurity has become a critical policy area in the 21 st century, transcending national borders and becoming intertwined with economic, social, and geopolitical issues. Many countries have

¹ *Коданева Светлана Игоревна*, ведущий научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук, доцент.

adopted their own legal frameworks in this area, although the specific approaches implemented may vary depending on local legal traditions and other factors. Regulatory acts in the information security field cover a wide range of topics, from laws protecting data and critical infrastructure to preventing cybercrime and protecting against information and psychological impacts. Based on an analysis of legal frameworks from various countries, this paper identifies general trends in the development of information security legislation.

Keywords: cybersecurity; data protection; protection of critical information infrastructure; information security; cyber sovereignty; cyber incidents.

Для цитирования: Коданева С.И. Правовое регулирование и институциональные основы информационной безопасности в России и в зарубежных странах (Статья) // Социальные и гуманитарные науки: Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 90–108. – DOI: 10.31249/iajpravo/2026.01.06

Введение

Глобальная цифровая трансформация, стимулируя беспрецедентный экономический рост и развитие социальных связей, привела к всеобщей зависимости от цифровой инфраструктуры. Оцифровка критически важных областей – от энергетических сетей и финансовых систем до здравоохранения и государственных услуг – в геометрической прогрессии усилила воздействие киберинцидентов на общество, поскольку их последствия носят все более массовый характер. Так, например, кибератаки привели к серьезным сбоям в работе ключевых коммунальных служб (таких как система газоснабжения из-за атаки вируса-вымогателя на трубопроводную компанию Colonial Pipeline в США в 2022 г. или попытка отравления водоочистных сооружений во Флориде, 2021 г.), морских портов (например DP World Australia, 2023 г.), банковских услуг (например банк Nonghyup в Южной Корее, 2011 г.), служб здравоохранения (например кибератака на немецкую больницу, приведшая к смерти пациента скорой помощи, 2020 г.)¹ и др.

Все эти примеры демонстрируют эволюцию характера как киберинцидентов, так и их организаторов – от хакеров-одиночек до преступных и террористических группировок и даже госу-

¹ Seng N. Cybersecurity Regulation – Types, Principles, and Country Deep Dives in Asia // International Cybersecurity Law Review. – 2024. – Vol. 5. – P. 87–411.

дарств, использующих подобные инструменты в своих гибридных войнах. Это превращает информационную безопасность из технической проблемы в ключевой вопрос национальной и общественной безопасности, а также экономической стабильности.

В ответ на этот растущий перечень угроз страны по всему миру активно принимают правовое регулирование, направленное на повышение уровня защищенности информации и критической инфраструктуры. Безусловно, подходы к регулированию довольно сильно различаются как по истории формирования, так и по структуре и лежащей в его основе философии. Однако наметилась тенденция к глобальной конвергенции этих разнообразных подходов вокруг нескольких ключевых принципов. Это сближение обусловлено общими вызовами: необходимостью защиты критической инфраструктуры, персональных данных, управления рисками цепочки поставок и развития международного сотрудничества в сфере, где злоумышленники действуют на международном уровне.

Национальные подходы к регулированию информационной безопасности

Правовое регулирование информационной безопасности в разных странах мира не только различается, как было отмечено выше, но и опирается на общие подходы, основанные на общих принципах. Помимо этого, в последнее время, как отмечает Э. Фахи, наметилась тенденция к конвергенции этих подходов даже в таких разных правовых порядках, как США и ЕС, что обусловлено единством угроз, с которыми сталкиваются все правительства¹.

В частности, представляется возможным выделить три группы нормативных правовых актов, регулирующих вопросы информационной безопасности:

1) законы, направленные на криминализацию противоправных действий в Интернете. Это форма правового регулирования исторически появилась одной из первых в ответ на случаи мошенничества, взлома и кибератак. Такие акты, как Закон США о компьютерном мошенничестве и злоупотреблениях (The Computer Fraud and Abuse Act, 1986), Закон Китая о кибербезопасности (The Cybersecurity Law of the People's Republic of China (Chinese:

¹ Fahey E. The Evolution of EU–US Cybersecurity Law and Policy: on Drivers of Convergence // Journal of European Integration. – 2024. – Vol. 46, N 7. – P. 1073–1088.

中华人民共和国网络安全法), 2016), Закон Индии об информационных технологиях (Information Technology Act, 2000) и Закон Соединенного Королевства о неправомерном использовании компьютеров (Computer Misuse Act, 1990), криминализируют несанкционированный доступ, повреждение и неправильное использование компьютерных систем. Однако слабостью данного подхода был трансграничный характер кибератак, в результате чего возникали проблемы юрисдикции;

2) законодательство, содержащее требования по управлению рисками и обеспечению устойчивости инфраструктуры. Эта категория представляет собой наиболее значительную и растущую область регулирования кибербезопасности, смещающую акцент с наказания злоумышленников на предписание владельцам информационной инфраструктуры принимать меры по защите конфиденциальности, целостности и доступности своих систем и данных, т.е. на предотвращение инцидентов. Подобного рода акты приняты во многих странах, включая Регламент ЕС № 2022/2555 о сетях и информационных системах (Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union), Закон Сингапура о кибербезопасности (Cybersecurity Act, 2018), Закон Австралии о безопасности критической инфраструктуры (Security of Critical Infrastructure Act, 2018) и др. Эти законы обычно определяют меры организационного и технического характера по защите данных и инфраструктуры;

3) законодательство, предписывающее отчитываться об инцидентах. Эта тенденция регулирования возникла позже двух предыдущих. Суть ее заключается в требовании, чтобы организации сообщали об инцидентах в области кибербезопасности государственным органам и, в некоторых случаях, общественности. Яркими примерами являются правила Комиссии по ценным бумагам и биржам США 2023 г., требования к отчетности в рамках указанного выше Регламента ЕС, а также инструкции по сертификации Индии. Цели данного рода актов двоякие: с одной стороны, повысить осведомленность органов власти о ландшафте киберугроз, а с другой – стимулировать компании повышать уровень и качество их информационной безопасности.

Соединенные Штаты Америки имеют сложную и фрагментированную систему регулирования кибербезопасности. Модель США характеризуется ориентацией на конкретный сектор, сочетанием полномочий федерального уровня и уровня штатов и акцентом на государственно-частное партнерство и частный сектор. Это

означает, что для ряда секторов специальными законами устанавливаются единые требования (например, Закон об управлении информационной безопасностью (Federal Information Security Management Act, 2002), уделяющий особое внимание безопасности систем федерального правительства; Закон о переносимости и подотчетности медицинского страхования (Health Insurance Portability and Accountability Act, 1996) устанавливает стандарты защиты конфиденциальной медицинской информации пациентов, Закон Грэмма-Лича-Блайли (Financial Services Modernization Act (Gramm-Leach-Bliley Act), 1999) обязывает финансовые учреждения разъяснять свои методы обмена информацией и защищать конфиденциальные данные клиентов и т.д.). В отношении остальных сфер применяются необязательные стандарты, хотя недавно принятый в 2022 г. Закон об отчетности о киберинцидентах для критической инфраструктуры (Cyber Incident Reporting for Critical Infrastructure Act, 2022) представляет собой значительный шаг на пути к более унифицированному стандарту отчетности для соответствующих объектов.

Наиболее значимой системой добровольной стандартизации является система кибербезопасности Национального института стандартов и технологий (National Institute of Standards and Technologies, NIST) – основанный на оценке рисков набор руководящих принципов, передовой практики и стандартов для управления рисками кибербезопасности. Показательно, что пять основных направлений, предложенных NIST (идентификация, защита, обнаружение, реагирование, восстановление), используются большинством стран мира и многими компаниями частного сектора как основа при создании собственных систем кибербезопасности.

Правоприменительная практика в США столь же фрагментирована, поскольку опирается на ведомственные акты или регулирование штатов. Все это, а также необходимость учитывать более жесткие обязательные стандарты, например ЕС, создает для американских компаний проблемы и сложности, хотя делает систему гибкой и адаптивной¹.

Европейский союз претендует на роль глобального центра регулирования в области кибербезопасности. Он придерживается всеобъемлющей, согласованной и быстро расширяющейся право-

¹ Assessing the Effectiveness of Current Cybersecurity Regulations and Policies in the US / E. Oluomachi, A. Ahmed, W. Ahmed, E. Samson // International Journal of Scientific and Research Publications. – 2024. – Vol. 14, N 2. – P. 78–85.

вой базы, основанной на приоритете прав человека. Правовую основу образуют Общий регламент по защите данных (General Data Protection Regulation 2016/679, GDPR, 2016)¹ и Директива по сетевой и информационной безопасности (Network and Information Security Directive (EU) 2022/2555, NIS2, 2022)².

Политика кибербезопасности ЕС прошла в своем развитии три этапа: генезис, институционализацию и «фазу регулирования». Этот третий этап, на котором ЕС находится сегодня, характерен тем, что кибербезопасность представлена как вопрос «европейского суверенитета». При этом реализуется концепция «нормативного меркантилизма»³, объединяющая вопросы экономики, безопасности и суверенитета и направленная не только на защиту внутреннего рынка, но и на распространение норм ЕС по всему миру. Соответственно, объем правотворчества активно растет в последние годы. В частности, принят Регламент ЕС 2019/881/EU о кибербезопасности (Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity), 2019), который закрепил мандат Агентства ЕС по кибербезопасности и создал общеевропейскую систему сертификации продуктов и услуг в области кибербезопасности. Также разработаны проекты регламентов о киберустойчивости (направлен на обеспечение того, чтобы продукты с цифровыми элементами (от интеллектуальных холодильников до промышленного программного обеспечения) продавались со встроенной сис-

¹ Хотя формально он касается персональных данных, но установленные в нем требования к безопасному хранению, передаче и обработке данных фактически оказали преобразующее влияние на кибербезопасность не только в ЕС, но и во всем мире, поскольку за нарушение этих требований предусмотрены серьезные штрафы в размере до 4% от мирового годового оборота компании – GDPR's Impact on Cybersecurity: A Review Focusing on USA and European Practices / O.O. Amoo, A. Atadoga, F. Osasona, T.O. Abrahams, B.S. Ayinla, O.A. Farayola // International Journal of Science and Research Archive. – 2024. – Vol. 11, N 1. – P. 1338–1347.

² Первый ее вариант, принятый в 2016 г., был адресован операторам основных услуг (OES) и поставщикам цифровых услуг (DSP), но новая Директива NIS2, принятая в 2022 г., значительно расширила сферу применения, охватывая гораздо более широкий круг секторов, включая энергетику, транспорт, банковское дело, здравоохранение, цифровую инфраструктуру и государственное управление, налагая строгие обязательства по управлению рисками, отчетности и обеспечению безопасности цепочки поставок.

³ Carrapico H., Farrand B. Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics // Journal of Common Market Studies. – 2024. – Vol. 62. – P. 147–158.

темой кибербезопасности, охватывающей весь их жизненный цикл), о киберсолидарности (направлен на создание «киберщита ЕС» из операционных центров безопасности и укрепление совместных возможностей обеспечения готовности к инцидентам и реагирования на них) и о цифровой операционной устойчивости (направлен на финансовый сектор, гарантируя, что он сможет противостоять всем типам сбоям и угроз, связанных с ИКТ).

Правоприменение в ЕС децентрализовано, но опирается на общие правила, устанавливающие как общие требования, так и меры наказания. Институциональную основу образует сеть органов, включая ENISA (которая обеспечивает экспертизу и координацию), национальные группы реагирования на инциденты компьютерной безопасности (National Computer Security Incident Response Teams (CSIRTs)) и компетентные органы в каждом государстве-члене. Однако увеличение объема нормативного регулирования и бюрократической нагрузки в сфере кибербезопасности ослабляют мотивацию к получению прибыли и мешают предпринимателям использовать инновационные решения в области безопасности, что тормозит их развитие. В результате компании направляют свою энергию от продуктивных инноваций в области безопасности к непродуктивному соблюдению формальных требований¹.

Российский подход к тому, что на Западе принято называть «кибербезопасностью», имеет существенные отличия. Он шире и глубоко интегрирован в парадигму национальной безопасности, воплощаясь в термине «информационная безопасность». Эта концепция выходит далеко за рамки технической защиты компьютерных систем и охватывает защиту национального суверенитета, социальной стабильности общества² и психологического благополучия населения от информационно-психологических манипуляций³.

Краеугольным камнем российского подхода является его доктринальная основа, которая определяет информацию как клю-

¹ Kianpour M., Raza Sh. More than Malware: Unmasking the Hidden Risk of Cybersecurity Regulations // International Cybersecurity Law Review. – 2024. – Vol. 5. – P. 169–212.

² Салов И.В., Байрушин Ф.Т., Абрамов И.Р. Информационная безопасность как фактор обеспечения социальной стабильности в российском обществе // Евразийский юридический журнал. – 2023. – № 8 (183). – С. 427–428.

³ Матюхин О.И. Информационная безопасность сквозь призму теории Джеймса Биллингтона: «Пожар в сознании» и угрозы цифровой эпохи // Вопросы безопасности. – 2025. – № 2. – С. 41–52.

чевой элемент национальной безопасности и вектор потенциальных угроз¹. При этом существует фундаментальное концептуальное расхождение между российским дискурсом «информационной безопасности» и западным дискурсом «кибербезопасности». Российский подход является более целостным, но сложным и спорным. Поэтому научные дебаты о содержании данного понятия до сих пор не стихают. Одни авторы анализируют состояние технической защищенности как таковой, включая противодействие кибератакам и проблематику защиты данных². Другие же основное внимание уделяют последствиям влияния неконтролируемого распространения информации на традиционные духовные ценности, состояние морали в обществе и национальную безопасность³. Так, М.В. Конохов связывает борьбу с «фейками» с национальной безопасностью, особенно в контексте СВО, утверждая, что ложная информация является ключевым инструментом информационных операций против России⁴. А.И. Толстой выделяет информационно-психологическую безопасность человека как самостоятельную область информационной безопасности и даже полагает, что данное понятие следует использовать исключительно для этой ориентированной на человека области, и что нынешнее широкое понимание информационной безопасности является исторической ошибкой при переводе международных стандартов⁵.

Некоторые авторы, в частности А.К. Дубень, опираясь на положения Стратегии национальной безопасности России, предла-

¹ Сосновская Ю.Н., Клементьева В.С. К вопросу о содержании информационной безопасности как приоритетного компонента национальной безопасности // Вестник экономической безопасности. – 2023. – № 6. – С. 156–161.

² Tereschenko L.K., Starodubova O.E., Nazarov N.A. New Information Technologies and Data Security. A review // Legal Issues in the Digital Age. – 2023. – Vol. 4, N 2. – P. 158–175; Пекарева В.В., Фроловская Ю.И. Конфиденциальность, целостность, доступность данных как основные принципы информационной безопасности // Аграрное и земельное право. – 2024. – № 4 (232). – С. 104–106.

³ Tsvyk V.A., Tsvyk I.V. Personal Information Security as a Social Problem // RUDN journal of sociology. – 2023. – N 23. – С. 590–599.

⁴ Конохов М.В. О некоторых вопросах правового обеспечения информационной безопасности Российской Федерации: международные и внутригосударственные аспекты // Право и государство: теория и практика. – 2024. – № 4 (232). – С. 173–176.

⁵ Толстой А.И. Обеспечение безопасности объектов в информационной сфере // Безопасность информационных технологий. – 2024. – Т. 31, № 3. – С. 105–123.

гают использовать комплексный подход, объединяющий под единым термином «информационная безопасность» как состояние защищенности в информационном пространстве, так и защиту конституционно значимых ценностей и суверенитета государства¹.

Как можно видеть, информационная безопасность в российском понимании включает:

– информационно-техническую безопасность (защиту информационных систем, сетей и данных от несанкционированного доступа, сбоя или уничтожения, что соответствует западной концепции кибербезопасности);

– информационно-психологическую безопасность (защиту индивидуального и общественного сознания от манипулятивного информационного воздействия, «фейков» и нарративов, дестабилизирующих общество, подрывающих традиционные ценности или дискредитирующих государственные институты и вооруженные силы);

– информационная безопасность как основа национальной безопасности (опирается на идею информационного суверенитета как состояния защищенности национальных и общественных интересов, интересов личности). Именно это понимание информационной безопасности Россия стремится продвигать на международном уровне в качестве концептуальной основы для международных соглашений и договоров с другими странами, стараясь с помощью юридически обязывающих соглашений ограничить информационные операции и распространение дестабилизирующего контента, чему западные страны сопротивляются, ссылаясь на свободу слова.

Российское законодательство является в высшей степени централизованным и детализированным. Его концептуальную основу составляют Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 05.12.2016 № 646, которая определяет четыре основные сферы национальных интересов (личность, общество, государство, стратегическое сдерживание); Стратегия национальной безопасности РФ, утвержденная Указом Президента РФ от 02.07.2021 № 400, согласно которой информационная безопасность является одним из ключевых компонентов национальной безопасности, а внешние информационные кампании представлены как угроза конституционному строю России, и

¹ Дубень А.К. Информационная безопасность: определение понятия, место в системе национальной безопасности // Аграрное и земельное право. – 2023. – № 11 (227). – С. 93–95.

обозначена необходимость защиты населения от деструктивных информационно-психологических воздействий; а также Концепция Государственной системы обнаружения, предотвращения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, утвержденная Указом Президента РФ от 12.12.2014 № К 1274, заложившая основу защиты и мер реагирования государства на киберинциденты, создав систему ГосСОПКА, за функционирование которой отвечает Федеральная служба безопасности РФ.

Положения этих стратегических концептуальных документов детализируются в федеральных законах: от 26.07.2017 (ред. 07.04.2025) № 187-ФЗ «О безопасности критически важной информационной инфраструктуры»; от 27.07.2006 (ред. от 24.06.2025) № 149-ФЗ «Об информации, информационных технологиях и защите информации»; от 27.07.2006 (ред. от 24.06.2025) № 152-ФЗ (ред. от 24.06.2025) «О персональных данных»; от 25.07.2002 (ред. от 27.10.2025) № 114-ФЗ «О противодействии экстремистской деятельности») и многочисленных подзаконных актах¹.

В целом в российской правовой системе используются подходы, схожие с европейскими, хотя и с большей степенью конкретизации и обязательности регулирования. Процесс защиты объектов критически важной информационной инфраструктуры является методичным и четким. Ее владельцы обязаны осуществлять категоризацию принадлежащей им инфраструктуры в зависимости от значимости для государственной безопасности, общественного порядка и экономической стабильности. Для наиболее значимых объектов разрабатывается система безопасности. Это не просто набор программного обеспечения, а интегрированная система, включающая технические (сертифицированное программное и аппаратное обеспечение), организационные (персонал, подразделения внутренней безопасности) и нормативные (политики, процедуры и планы) элементы. Кроме того владелец инфраструктуры должен выполнять набор мер, утвержденный ФСТЭК, которая проводит постоянные проверки, и подключаться к системе ГосСОПКА.

¹ Подробнее см.: Структура действующих нормативных правовых актов в области обеспечения безопасности объектов критической информационной инфраструктуры Российской Федерации / А.В. Бондаренко, К.В. Мушовец, С.В. Поршнев, О.К. Рогова // Безопасность информационных технологий. – 2023. – Т. 30, № 3. – С. 126–148.

Учитывая сложность и обширность правовой базы, касающейся информационной безопасности, в России сложилась сложная система уполномоченных органов: Минцифры России отвечает за широкий сектор информационных технологий и телекоммуникаций, регулирует безопасность сетей связи общего пользования, которые эксплуатируются значимыми объектами критически важной инфраструктуры. Оно выпускает рекомендации по сертификации коммуникационного оборудования и организационно-техническим мерам обеспечения сетевой безопасности. Федеральная служба по техническому и экспортному контролю (ФСТЭК) обеспечивает защищенность критически важной информационной инфраструктуры, также как ФСБ России, пользующаяся системой ГосСОПКА и управляющая ею, обеспечивающая сертификацию инфраструктуры, лицензирование криптографической деятельности, координирующая реагирование на инциденты на объектах критически важной инфраструктуры.

Правоохранительные органы также принимают участие в обеспечении информационной безопасности. Так, прокуратура осуществляет надзор за законностью деятельности указанных выше государственных органов, включая ФСБ России и ФСТЭК, а также частных организаций в области информационной безопасности¹. Полиция осуществляет контроль за соблюдением законодательства в области информационной безопасности предприятиями и гражданами, налагает штрафы за административные правонарушения в данной сфере, а также занимается пропагандой и повышением осведомленности, информируя общественность об информационных угрозах (например видеоролики в метро о киберпреступности)².

Кроме того, Роскомнадзор и прокуратура наделены полномочиями по контролю за распространяемой в сети Интернет информацией.

В то же время Россия сталкивается с серьезными проблемами в данной сфере. Прежде всего, это зависимость от западных

¹ Соколов И.А. Особенности определения пределов деятельности прокуратуры по обеспечению информационной безопасности государства // *Власть закона*. – 2023. – № 3 (55). – С. 338–350.

² Федорова И.В., Калинина С.В., Самохвалов В.В. Особенности административной деятельности полиции в сфере обеспечения информационной безопасности // *Вестник московского университета МВД России*. – 2023. – № 6. – С. 238–242.

технологий, уход западных компаний из страны и санкции¹. На решение этих проблем направлены Указ Президента РФ от 30.03.2022 (ред. 07.04.2025) № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», запрещающий госзаказчикам закупать иностранное программное обеспечение при наличии российских альтернатив, внесенные в Гражданский кодекс РФ и узаконившие параллельный импорт критически важных для страны технологий, а также комплекс мер, направленных на поддержку отечественных разработчиков и производителей ИТ-технологий.

Таким образом, нормативно-правовая база РФ по информационной безопасности является всеобъемлющей, детализированной и постоянно развивается. Она основана на следующих принципах: холизм²; суверенитет; централизация; устойчивость к киберинцидентам; обязательность государственного регулирования (в противовес американской модели саморегулирования).

Эта система не лишена внутренних противоречий и проблем, однако она представляет собой последовательную и целенаправленную стратегию управления рисками и использования возможностей информационной эпохи на своих собственных условиях.

Азиатско-Тихоокеанский регион демонстрирует широкий спектр подходов, от достаточно хорошо развитых моделей Китая, Сингапура, Японии и Австралии и до развивающихся структур Индонезии.

Подход *Китая* к регулированию кибербезопасности основан на принципе киберсуверенитета (утверждении абсолютного национального контроля над Интернетом в пределах своих границ), что резко контрастирует с западными моделями. Эти различия носят не только технический, но и философский характер, оказывая влияние на все – от управления данными и защиты критически важной инфраструктуры до самого определения безопасности, ко-

¹ Вершинин А.Н. Цифровая трансформация информационной безопасности критической информационной инфраструктуры в условиях импортозамещения // Научный аспект. – 2023. – Т. 2, № 5. – С. 209–217.

² Отказ от узкой модели «кибербезопасности» в пользу целостной парадигмы «информационной безопасности», которая объединяет техническую и психологическую защиту.

торое в Китае включает в себя не только техническую целостность, но и политическую и социальную стабильность¹.

В Китае система регулирования вопросов информационной безопасности действует по принципу «сверху вниз» и имеет двоякую цель – обеспечение национальной безопасности и стабильности режима. основополагающим является Закон о кибербезопасности (The Cybersecurity Law of the People's Republic of China (Chinese: 中华人民共和国网络安全法), 2016), базирующийся на принципе сочетания кибернетического суверенитета (предоставляющего государству широкие полномочия по регулированию и контролю интернет-инфраструктуры и контента) и «безопасных и контролируемых» сетей (расплывчатый термин, который интерпретируется как предписывающий использование отечественных технологий для снижения зависимости от иностранных поставщиков, что позволяет получать доступ ко всем данным органам власти для обеспечения государственной безопасности). Этот закон, как и во многих других странах, основное внимание уделяет защите критически важной информационной инфраструктуры. Однако китайское определение включает в себя «общественные коммуникационные и информационные службы» и «другие важные сферы, которые в случае разрушения, потери функций или утечки данных могут серьезно угрожать национальной безопасности, национальному благосостоянию, средствам к существованию людей или общественным интересам», что фактически ставит под государственный контроль практически всю цифровую экономику страны. Помимо этого, закон содержит требование локализации данных и существенные ограничения по их трансграничной передаче. Эти нормы значительно строже, чем в ЕС, поскольку передача личной информации за рубеж возможна только «по требованию бизнеса» и подлежит обязательной оценке безопасности, проводимой Управлением по киберпространству Китая (Cyberspace Administration of China, САС). Закон также обязывает сетевых операторов требовать от пользователей предоставления реальных идентификационных данных, что фактически прекращает анонимность в Интернете. Это является уникальной отличительной чертой китайской модели, отсутствующей в других рассмотренных правовых моделях.

¹ Creemers R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy // Journal of Contemporary China. – 2024. – Vol. 33, N 146. – P. 173–188.

В дополнение к Закону о кибербезопасности в Китае приняты Закон о защите данных (Data Security Law of the People's Republic of China (Chinese: 中华人民共和国数据安全法) (DSL), 2021) и Закон о защите личной информации (Personal Information Protection Law of the People's Republic of China (Chinese: 中华人民共和国个人信息保护法) (PIPL), 2021). Первый создает систему секретной и дифференцированной защиты всех данных, основанную на их важности для национальной безопасности и общественных интересов. Это еще больше расширяет возможности государства по контролю за данными и доступу к ним, создавая правовую основу для наказания за действия, которые считаются наносящими ущерб государственной безопасности. Второй, часто называемый «Общим регламентом по защите данных Китая», предоставляет гражданам страны право на конфиденциальность. Однако это право в значительной степени ограничено исключениями, касающимися национальной безопасности и общественных интересов и требованием к операторам данных сотрудничать с органами общественной безопасности и ведомствами госбезопасности.

На подзаконном уровне в Китае принята Многоуровневая схема защиты (Multi-Level Protection Scheme (MLPS 2.0), 2020), которая требует от всех сетевых операторов в Китае классифицировать свои системы по одному из пяти уровней безопасности, и применять соответствующие меры защиты. В целом система похожа на американскую систему NIST, но в отличие от нее является обязательной.

Основным правоприменительным органом в рассматриваемой сфере является Управление по киберпространству Китая – влиятельный партийный орган, обладающий широкими полномочиями. Его решения не подлежат судебному пересмотру. Помимо этого Положение о надзоре и проверке интернет-безопасности органами общественной безопасности 2018 г. наделило правоохранительные органы полномочиями на доступ (в том числе удаленный) и копирование данных, имеющих отношение к кибербезопасности.

Китай не просто разрушает западную модель глобального и открытого Интернета у себя в стране, но активно экспортирует свою модель «кибернетического суверенитета» через такие площадки, как ООН, и через свою инициативу «Цифровой шелковый путь», предлагая альтернативу западной либеральной модели управления Интернетом. Следует отметить, что вопросы информационной безопасности становятся инструментом не только в

информационной войне между США и Китаем, но и конкурентных войн между транснациональными корпорациями этих двух стран. Причем эти два аспекта очень тесно переплетены, делая вопросы кибербезопасности политическими. Например, в 2024 г. в США был принят Закон о защите американцев от приложений, контролируемых иностранными противниками (Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA), 2024), направленный против TikTok, согласно которому социальная сеть или должна быть продана американской компании, или будет заблокирована. Правительство Китая предпочло второй вариант¹.

Стратегия кибербезопасности *Сингапура* 2021 г. отличается ясностью, централизацией и нацеленностью на технологическое развитие. Она включает четыре основных компонента: создание устойчивой инфраструктуры, создание безопасного киберпространства, развитие динамичной экосистемы кибербезопасности и укрепление международных партнерств. Правовую основу информационной безопасности в этой стране составляет Закон о кибербезопасности 2018 г., который предоставляет Агентству кибербезопасности (Cyber Security Agency of Singapore, CSA) широкие полномочия в отношении защиты критической информационной инфраструктуры в 11 ключевых секторах. Закон содержит «Кодекс практики», в котором излагаются конкретные технические и организационные требования к владельцам инфраструктуры, охватывающие управление, защиту, обнаружение, реагирование и восстановление. Закон о защите персональных данных (Personal Data Protection Act (PDPA) 2012), как и его европейский аналог, включает требования относительно разумных мер безопасности персональных данных. Комиссия по защите персональных данных (Personal Data Protection Commission, PDPC) приняла множество решений, которые содержат практические рекомендации касательно того, что считается «разумным». Денежно-кредитное управление Сингапура (Monetary Authority of Singapore, MAS) выпускает обязательные уведомления по управлению технологическими рисками и кибергигиене для финансового сектора, создавая надежный уровень регулирования для этого сектора.

Таким образом, в Сингапуре реализован смешанный подход: Закон о защите персональных данных содержит принципы обеспе-

¹ Петрунин Ю.Ю., Бухарин В.В. От информационной безопасности к национальной: противоборство IT-компаний США и КНР // Безопасность цифровых технологий. – 2024. – № 2 (113). – С. 25–54.

***Правовое регулирование и институциональные основы
информационной безопасности в России и в зарубежных странах***

чения их безопасности для всех операторов данных, Закон о кибербезопасности и принятые в его развитие акты CSA устанавливают четкие предписания для владельцев критической инфраструктуры, что сочетается с отраслевым подходом в деятельности MAS.

Система *Японии* основана на сочетании законов, содержащих общие принципы и нормы (Закон о защите личной информации (The Act on the Protection of Personal Information (APPI), 2003), требует от предприятий принимать «необходимые и уместные» меры безопасности; Закон о телекоммуникационном бизнесе (Telecommunications Business Act (TBA), 1984) содержит требования по кибербезопасности для операторов связи, включая разработку «правил обращения с информацией», назначение главного контролера и ежегодные самооценки, и подробные, но не имеющие обязательной силы рекомендации регулирующих органов. Таким образом, японская система сочетает в себе общие подходы к регулированию на уровне законов, закладывающие основу для правоприменительной сферы, с гибкостью, обеспеченной подробностью, но необязательностью подзаконных рекомендаций.

В *Австралии* основу правового регулирования составляют Австралийская стратегия и план действий в области кибербезопасности на 2023–2030 гг. и Закон о безопасности критически важной инфраструктуры (Security of Critical Infrastructure Act (SOCI), 2018); использованный в нем подход похож на российскую модель – на владельца критически важной инфраструктуры наложено «позитивное обязательство по обеспечению безопасности», включающее требование по принятию программы управления рисками для критически важной инфраструктуры (Critical Infrastructure Risk Management Programs (CIRMP)), основанной либо на стандартах NIST, либо на «модели зрелости» Австралийского управления сигналами «Essential Eight»¹. Это гибридный подход: обязательные стандарты без чрезмерной детализации. Кроме того, Закон о неприкосновенности частной жизни (The Privacy Act, 1988) налагает обязательство предпринимать «разумные шаги» для защиты личной информации, соблюдение которых обеспечивается Управлением Австралийского комиссара по информации (Oaic).

Правовой ландшафт *Индонезии* в области кибербезопасности является символом проблем, с которыми сталкиваются многие

¹ Digital Resilience. International and Domestic Legal Responses to Cyber Security and Artificial Intelligence / eds. D. Stephens, M. Stubbs, S. White. – Singapore: Springer Nature Singapore, 2025. – 209 p.

развивающиеся цифровые экономики. Закон об электронной информации и транзакциях (Law on Electronic Information and Transactions (ITE Law), 2008) обеспечивает правовую основу, криминализируя киберпреступность и устанавливая принципы электронных транзакций. Однако в целом нормативно-правовая база раздроблена на множество законов, актов правительства и министерств. При этом полномочия Министерства связи и информации, Национального агентства по кибербезопасности и криптографии и полиции частично совпадают. Индонезийское общество плохо информировано о вопросах информационной безопасности и связанных с ней рисках. Ресурсы как органов власти, так и компаний крайне ограничены, что не позволяет им реализовать полноценные системы киберзащиты. Основной проблемой является нехватка квалифицированных кадров¹.

В системах *Индии* и *Пакистана* акцент смещен на криминализацию цифровых атак и кибертерроризма. Закон Индии об информационных технологиях (Information Technology Act, 2000) направлен на борьбу с киберпреступностью, также как и Закон Пакистана о предотвращении электронных преступлений (Prevention of Electronic Crimes Act, 2016)².

Заключение

Как можно видеть, несмотря на существующие различия в правовых подходах к регулированию информационной безопасности, можно обнаружить и ряд сходств:

1. Важность защиты критически важных объектов инфраструктуры (существует общее признание того, что определенные сектора настолько жизненно необходимы, что киберинциденты на них представляют угрозу национальной безопасности, поэтому законодательство всех стран направлено на защиту такой инфраструктуры, хотя масштабы регулирования и конкретные обязательства различаются).

¹ Rhogust M. Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia // Journal of Law, Social Science and Humanities. – 2024. – Vol. 1, N 2. – P. 166–180.

² A Survey of Cybersecurity Laws, Regulations, and Policies in Technologically Advanced Nations: a Case Study of Pakistan to Bridge the Gap / B. Saleem, M. Ahmed, M. Zahra, F. Hassan, M.A. Iqbal, Z. Muhammad // International Cybersecurity Law Review. – 2024. – Vol. 5. – P. 533–561.

2. Рост числа обязательных отчетов об инцидентах (переход от добровольного обмена информацией к обязательному своевременному сообщению о значительных инцидентах в настоящее время является глобальным трендом даже в таких странах, как США).

3. Цепочка поставок и управление рисками сторонних производителей (не только для России важно обеспечение бесперебойных поставок качественного оборудования, другие страны также озабочены данной проблемой, что отражается в их законодательстве: например, указы президента США о безопасности цепочки поставок программного обеспечения или «Кодекс практики» Сингапура налагают обязательства по управлению рисками на поставщиков и сервис-провайдеров).

4. Влияние системы NIST (хотя эта система стандартизации и является рекомендательной и добровольной в США, но де-факто она стала глобальным стандартом кибербезопасности).

5. Слияние защиты данных и кибербезопасности (принятие GDPR стало поворотным моментом в правовых подходах к кибербезопасности – все больше стран мира рассматривают данную область через призму защиты персональных данных).

Основными принципами информационной безопасности, которых придерживаются большинство стран мира, являются:

1. Регулирование, основанное на оценке рисков: требования должны быть пропорциональны ущербу, который может нанести инцидент в области кибербезопасности. Возлагать одинаковое бремя на международный банк и мелкого розничного продавца неэффективно. Поэтому правовое регулирование, как правило, направлено на операторов критически важной информационной инфраструктуры или «основных услуг» (организации в таких секторах, как энергетика, водоснабжение, финансы, здравоохранение и транспорт, где последствия сбоя могут иметь опасные последствия для всего общества, повлечь существенный экономический ущерб).

2. Технологическая нейтральность: нормативные акты содержат только требования к результату принимаемых мер (например, «обеспечивать безопасность»), но не к используемым для этого технологиям (например «использовать шифрование AES-256»). Этот принцип отражает то, что технологии очень быстро развиваются и устаревают, поэтому технологическая нейтральность правового регулирования позволяет организациям адаптировать свои средства защиты к возникающим угрозам и инновациям.

3. Отказ от чрезмерно детализированного регулирования и фрагментации: чрезмерно подробные правила могут быть негибкими и не учитывать уникальный контекст организации. Более того, когда разные страны принимают совершенно разные требования, это создает дополнительную нагрузку на транснациональные корпорации, вынужденные подстраиваться под множество национальных правовых порядков. Соответственно, некоторые страны предпочитают закреплять только общие положения и принципы, которые могут способствовать международной гармонизации правового регулирования. Однако, как было показано выше, этот принцип не является универсальным, поскольку такие страны, как Китай и Россия, напротив, стремятся защитить свой киберсуверенитет, в том числе посредством детализации и фрагментации правового пространства.

4. Приоритет в законодательстве мер стимулирования использованию передовых практик перед криминализацией: эффективное правовое регулирование нацеливает организации внедрять самые современные и передовые подходы к информационной безопасности, применяя для этого различные меры стимулирования. Например, Закон США об обмене информацией о кибербезопасности (Cybersecurity Information Sharing Act, 2015) предоставляет юридические убежища компаниям, делящимся с органами власти данными о киберугрозах, тем самым укрепляя коллективную защиту.