DOI https://doi.org/10.24866/VVSU/2073-3984/2021-1/115-124

УДК 341.171

Э.В. Горян

Владивостокский государственный университет экономики и сервиса
Владивосток. Россия

Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики*

Объектом исследования являются отношения, возникающие при осуществлении мер по обеспечению кибербезопасности. Характеризуются положения Стратегии национальной безопасности в киберпространстве КНР как ключевого документа, определяющего систему кибербезопасности. С целью получения наиболее достоверных научных результатов использованы нормативно-правовой и сравнительно-правовой методы. КНР в своих стратегических документах определяет основные информационные угрозы во внутренней и внешней сфере, а также приоритеты развития системы кибербезопасности, уделяя внимание балансу интересов государства и прав личности, формированию и развитию в положительном русле цифровой культуры граждан. Особенностью национальной стратегии кибербезопасности КНР является использование термина «киберпространство» в качестве объекта регулирования. Следует рассмотреть возможность закрепления дефиниции киберпространства, используемой в КНР, в российском законодательстве. Важным аспектом китайской стратегии является определение граждан как активных субъектов информационного пространства с последующим установлением их правового статуса в отношениях обеспечения кибербезопасности и возложением на них соответствующей ответственности. Преимуществом китайской стратегии кибербезопасности является акцент на государственно-частном партнерстве, в то время как в России основная ответственность возложена на государственно-публичный сектор. Необходимо рассмотреть внедрение этого подхода в России для более активного привлечения частного сектора (деловых кругов и граждан) к обеспечению кибербезопасности.

Ключевые слова и словосочетания: кибербезопасность, национальный механизм, Китай.

Горян Элла Владимировна – канд. юрид. наук, доцент, доцент кафедры гражданско-правовых дисциплин; e-mail: ella.goryan@vvsu.ru

* *Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 20-011-00454 «Обеспечение прав инвесторов в банковском и финансовом секторах в условиях цифровизации экономики в РФ и ведущих финансовых центрах Восточной Азии: сравнительно-правовой аспект».*

E.V. Gorian

Vladivostok State University of Economics and Service
Vladivostok. Russia

The legal framework for national security in cyberspace: the outcomes of the People's Republic of China

The provisions of the National Security Strategy in cyberspace of the PRC as a key document defining the cyber security system are characterized. In order to obtain the most reliable scientific results, the system-structural, formal-logical and formal-legal methods were used. In its strategic documents China defines the main information threats in the internal and external spheres, as well as the priorities for the development of the cyber security system, paying attention to the balance of the interests of the state and individual rights, as well as special attention to the formation and development in a positive direction of the digital culture of citizens. A feature of the national cybersecurity strategy of the PRC is the use of the term "cyberspace"; it also separately distinguishes citizens as active subjects of the information space, determining their share of responsibility for its security.

Keywords: cybersecurity, national mechanism, China.

Актуальность темы исследования

Последние годы государства активизируют свою деятельность по защите информационного пространства. Информационно-коммуникационные технологии как неотъемлемая часть государства и общества используются во всех сферах экономики. Человечество стало зависеть от этих технологий во всех аспектах своей жизни. Кибератаки на информационные системы учреждений здравоохранения, банковские и финансовые учреждения показали уязвимость привычного уклада жизни людей и государства в целом перед непредвиденными вызовами.

В 2011 году Россия выступила с инициативой разработки и принятия международного механизма обеспечения кибербезопасности, предложив свою концепцию Конвенции об обеспечении международной информационной безопасности. Однако эта инициатива не получила широкой поддержки из-за существующих разногласий по поводу участников такого механизма, их полномочий, особенностей международного сотрудничества и т.д. Тенденции таковы, что обеспечение кибербезопасности является задачей, прежде всего, национального масштаба, а международные механизмы формируются на региональном уровне, в рамках международных межправительственных организаций (например, АСЕАН) [2, с. 58] и наднациональных образований (Европейский союз). Инициатива в такой сфере принадлежит одному-двум государствам, которые играют лидирующую роль в интеграционных процессах и являются наиболее развитыми с точки зрения информационных технологий. Поэтому сегодня так называемая «гонка вооружений» переместилась из военно-промышленной сферы в информационную: каждое государство стремится разработать и усовершенствовать свой национальный механизм кибербезопасности, чтобы защитить свои интересы как в политической, так и экономической сферах.

В продолжение последних пяти лет Российская Федерация и Китайская Народная Республика особенно активно формируют свои системы кибербезопасности: разрабатывается нормативная база, совершенствуется система государственных органов, уполномоченных разрабатывать и принимать меры по кибербезопасности. Информационно-коммуникационные системы используются не только для совершения посягательств на экономическую систему государства, но и для влияния на политическую систему государства, вплоть до внешней политики. Указанные государства являются сторонниками так называемой «национальной» модели Интернета, предусматривающей активное участие государства в регулировании отношений в информационном пространстве, что определяет соответствующую модель механизма кибербезопасности. Изучение зарубежного опыта весьма важно для совершенствования российского национального механизма обеспечения кибербезопасности. Это и определяет актуальность темы нашего исследования.

Цель исследования – охарактеризовать национальную стратегию кибербезопасности Китая и выделить ее преимущества для внесения предложений в соответствующее российское законодательство.

С целью получения наиболее достоверных научных результатов использованы системно-структурный, формально-логический и формально-юридический методы.

Предмет исследования составляет Стратегия национальной безопасности в киберпространстве Китая 2016 года.

Выбранная нами тема мало исследована в российской научной литературе. Поиск в электронной библиотеке научных публикаций eLibrary.ru проиндексированных в РИНЦ исследований по теме выявил несколько статей, косвенно затрагивающих тему исследования и посвященных политическим аспектам кибербезопасности [5; 7; 9], а также в сравнительно-правовом плане [1]. Ученые отмечают, что в современной «нормативно-правовой системе КНР прослеживается тенденция замены действующей ограничительной модели на модель постепенного «открытия» китайского информационного сегмента. Это связано с необходимостью включения Китая в мировые информационно-финансовые процессы» [8, с. 165], а понимание информационной безопасности включает два аспекта: «одновременно и защиту ключевой инфраструктуры от кибератак, и фильтрацию контента в рамках внутренней сети. Во многом противоречия КНР и других стран мира связаны с тем, что Китай настаивает на исключительном праве на регулирование Интернета на территории страны, активно использует цензуру для фильтрации контента, запрещенного законодательством КНР и представляющего угрозу для имиджа страны и правящей партии» [6, с. 391]. Особенность китайского подхода к пониманию основных категорий кибербезопасности обусловливает уникальность национального механизма кибербезопасности.

Основная часть

В конце 2016 года был принят ключевой для Китайской Народной Республики документ, определивший основное направление внутренней и внешней политики в сфере информационной безопасности: Стратегия национальной безо-

пасности в киберпространстве [10]. Стратегия разрабатывалась и принималась одновременно с Законом Китайской Народной Республики о кибербезопасности [3], и оба документа стали результатом двухлетней работы китайского законодателя по реформированию механизма обеспечения кибербезопасности, вызванного широким применением информационных технологий, ростом и развитием киберпространства. Следует остановиться на определении киберпространства, данном в Стратегии: это пространство, состоящее из Интернета, телекоммуникационных сетей, компьютерных систем, автоматизированных систем управления, цифрового оборудования и приложений, услуг и данных. Но Концепция стратегии кибербезопасности Российской Федерации определяет киберпространство как сферу деятельности в информационном пространстве, образованную совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства) [4]. На наш взгляд, российское определение киберпространства размывает объект регулирования путем включения в непосредственные объекты кибербезопасности еще и «любые формы осуществляемой посредством их использования человеческой активности (личности, организации, государства)».

В преамбуле отмечена важность стратегии для реализации целей национальных программ, объявленных Си Цзиньпином: «Два столетия», «Четыре принципа» и «Пять точек зрения», направленных на усиление роли Китая в международном киберпространстве, процветание нации и защиту суверенитета. Стратегия состоит из четырех разделов. Первый раздел «Возможности и вызовы» характеризует основные возможности и серьезные вызовы, стоящие перед государством. К первым отнесены: 1) новые каналы распространения информации; 2) новые пространства для производства и жизни; 3) новые стимулы экономического развития; 4) новые носители культурного процветания; 5) новые платформы для социального управления; 6) новые точки взаимодействия и сотрудничества и 7) новые территории, на которые распространяется национальный суверенитет (киберпространство).

В качестве серьезных вызовов, с которыми сталкивается КНР, отмечены риски и проблемы в национальной политике, экономике, культуре, обществе, национальной обороне, безопасности и законных правах и интересах граждан в киберпространстве: а) кибервмешательство во внутреннюю политику, разжигание социальных волнений, кибершпионаж; б) кибератаки на критически важную информационную инфраструктуру, что представляет риск для экономической безопасности; в) распространение вредной информации онлайн, подрывающее культурную безопасность; г) киберпреступность (экстремизм, терроризм, сепаратизм, компьютерные преступления); д) международная борьба за контроль над стратегическими ресурсами в киберпространстве, за установление нормативной власти и реализацию стратегической инициативы [10].

Второй раздел стратегии посвящен целям развития механизма кибербезопасности. К ним отнесены: 1) достижение международного мира и безопасности путем сдерживания гонки вооружений в киберпространстве и недопущения злоупотребления информационными технологиями, а также конфликтов; 2) достижение безопасности киберпространства путем эффективного контроля рисков кибербезопасности, создания и совершенствования национальных систем обеспечения кибербезопасности, организации стабильной и надежной работы информационных систем; 3) достижение целей устойчивого развития, в том числе открытости и доступности цифровых технологий среди всех слоев общества и всех участников международного сообщества (особенно развивающихся стран), должны иметь возможность совместно использовать возможности развития, участвовать в результатах развития и справедливо участвовать в управлении киберпространством. И, наконец, последней целью было определено укрепление законности и международного правопорядка, достигаемое путем реализации и защиты прав и основных свобод человека и гражданина, а также путем создания международных нормативно-правовых и институциональных механизмов (раздел II) [10].

Третий раздел стратегии раскрывает содержание принципов, на которых строится внутренняя и внешняя политика кибербезопасности. К ним относятся: принцип уважения и защиты суверенитета в киберпространстве; принцип мирного использования кибепространства; принцип верховенства права и принцип комплексного управления кибербезопасностью и развитием (раздел III) [Там же].

Четвертый раздел стратегии посвящен определению стратегических задач, стоящих перед китайским государством. Рассмотрим их подробнее. В качестве первой задачи определена решительная защита суверенитета в киберпространстве. Для этого необходимо осуществлять управление деятельностью в киберпространстве на основе законодательства КНР, обеспечивать активную защиту информационной инфраструктуры и информационных ресурсов, а также принимать все меры, включая экономические, административные, научные, технологические, юридические, дипломатические и военные для защиты суверенитета в киберпространстве, одновременно противодействуя всем действиям, направленным на подрыв государственного режима или ограничение суверенитета.

Вторая задача заключается в обеспечении национальной безопасности путем 1) предотвращения, пресечения и преследования в рамках закона любого акта использования сети для совершения государственной измены, сепаратизма, подстрекательства к восстанию или подрывной деятельности или подстрекательства к свержению государственного режима; 2) предотвращения, пресечения и преследования в рамках закона действий, связанных с использованием сети для кражи или утечки государственной тайны, а также других действий, наносящих ущерб национальной безопасности; 3) предотвращения, пресечения действий и привлечения к ответственности на основе норм международного права иностранных государств, использующих сеть для проникновения, разрушения, подрывной и сепаратистской деятельности.

Третьей задачей определена защита национальной критической информационной инфраструктуры, влияющей на национальную безопасность, национальную экономику и благосостояние населения. Стратегия дает приблизительный перечень секторов критической информационной инфраструктуры: общественные телекоммуникации, радио- и телевещание, энергетика, финансы, транспорт, образование, научные исследования, гидроэнергетика, промышленность и производство, здравоохранение и медицина, социальное обеспечение, общественные предприятия. Особо отмечено, что защита критически важной информационной инфраструктуры является общей обязанностью правительства, бизнеса и всего общества, контролирующие и оперативные рабочие подразделения и организации должны в соответствии с требованиями законов, нормативных актов, правил и стандартов принимать своевременные меры для обеспечения безопасности важной информации. Тем не менее, жесткий механизм защиты критической информационной инфраструктуры должен функционировать в открытой среде. Необходимо создание и внедрение инструментов проверки кибербезопасности, усиление управления безопасностью цепочки поставок, запуск проверок безопасности для важных продуктов и услуг в области информационных технологий, приобретаемых и используемых в партийных и государственных органах, а также в целевых секторах, повышение безопасности и управляемости продуктов и услуг, предотвращение выпуска продукции поставщиками услуг и другими организациями, использующими свое преимущество в информационных технологиях для ненадлежащей конкуренции или во вред интересам пользователей [10].

Четвертая задача заключается в укреплении онлайн-культуры и онлайн-идеологии через всемерное поощрение социалистических взглядов на основные ценности, реализацию проектов создания сетевого контента и развитие позитивной онлайн-культуры. Для этого необходимо создавать новые онлайн-продукты и услуги, расширять цифровизацию процессов, содействовать обмену и взаимному ознакомлению китайской и иностранной культур. Целесообразно усилить нравственное воспитание, противодействовать распространению в сети слухов, насилия, суеверий, ереси и другой незаконной и вредоносной информации, обращая особое внимание на несовершеннолетних и молодежь.

Пятая цель – борьба с кибертерроризмом, кибершпионажем и компьютерной преступностью (мошенничество, посягательство на персональные данные, незаконный оборот оружия и наркотиков, распространение непристойных материалов, взлом компьютерных систем, нарушение прав интеллектуальной собственности и проч.).

В качестве шестой цели стратегии было определено совершенствование механизма управления киберпространством, которое достигается благодаря совершенствованию нормативной (законодательство) и институциональной систем обеспечения кибербезопасности вместе с повышением научного и стандартизованного уровня управления кибербезопасностью, а также посредством соблюдения законов, распространения правовых знаний среди населения. Насущным вопросом является ускорение создания системы управления сетью, сочетающей

в себе правовые нормы, административный надзор, отраслевую самодисциплину, технологическую защиту, массовый надзор и социальное просвещение, продвижение и управление инновациями и социальными онлайн-организациями, базовое управление, управление контентом. Одновременно следует усилить защиту тайны переписки, свободы слова, коммерческой тайны, а также права на репутацию, право собственности и другие законные права и интересы в киберпространстве. Все эти меры необходимо осуществлять с привлечением общественных организаций к участию в управлении сетью, обеспечивая развитие общественных мероприятий и укрепляя новые социальные организации в сети. Также пользователи сети могут сообщать о незаконных действиях и вредоносной информации в Интернете [10].

Седьмая цель стратегии охватывает сферу сетевой безопасности, обеспечение которой возможно при выполнении нескольких задач: 1) реализация политики, благоприятной для технологических инноваций;)2 поиск поддержки и поощрение частного сектора с интеграцией индустрий в систему кибербезопасности; 3) достижение прорыва в ключевых технологиях.

Реализация четвертой задачи возложена на разработчиков программного обеспечения: ускорение распространения и применения безопасных и надежных продуктов, развитие сетевой инфраструктуры и обогащение информационного контента в киберпространстве.

Пятая задача охватывает сферу электронной коммерции и больших массивов данных (big data), облачные вычисления и технологии нового поколения.

Отдельным блоком при достижении седьмой цели стоит совершенствование национальной системы поддержки технологий кибербезопасности: расширение исследований по основам теории и основным вопросам кибербезопасности; усиление работы по стандартизации, аутентификации и аккредитации в области кибербезопасности; многоуровневая защита, оценка рисков и обнаружение слабых мест, своевременное предупреждение и разработка механизмов экстренного реагирования на крупные инциденты кибербезопасности.

Влияние на человеческое измерение предусмотрено в стратегии путем реализации проекта подбора и подготовки специалистов в области кибербезопасности и финансирования научных профилей кибербезопасности, в том числе путем создания первоклассных академий кибербезопасности и инновационных парков, а также среды, благоприятной для развития талантов, инноваций и стартапов. Большое внимание государство уделяет пропаганде кибербезопасности среди населения, цифровой грамотности и вовлечению широких слоев населения в борьбу с незаконной и вредоносной информацией, онлайн-мошенничеством и другими преступными действиями.

Восьмая цель концентрируется на защите киберпространства как части государственной территории путем создания средств защиты кибербезопасности, своевременного обнаружения и противостояния кибератакам с помощью созданных надежных резервных сил для защиты национальной кибербезопасности.

И, наконец, девятая цель стратегии фокусируется на укреплении международного сотрудничества в рассматриваемой сфере путем углубления двусторонних и многосторонних диалогов по кибербезопасности, обмена информацией с другими государствами, активного участия в глобальных и региональных организациях, содействия в интернационализации управления интернет-адресами, серверами доменных имен и другими базовыми ресурсами. Китайская Народная Республика высоко оценивает деятельность Организации Объединенных Наций и поддерживает разработку на ее платформе международных общепризнанных норм для регулирования киберпространства, а также международного договора о борьбе с терроризмом в киберпространстве и других механизмов борьбы с киберпреступностью. Международное сотрудничество предполагает оказание всемерной поддержки развивающимся странам и привлечение новых участников проекта «Один пояс, один путь» в том числе в секторе информационно-коммуникационных технологий (раздел IV) [10].

Выводы. В результате проведенного исследования мы пришли к следующим выводам. КНР в своих стратегических документах определяет основные информационные угрозы во внутренней и внешней сфере, а также приоритеты развития системы кибербезопасности, уделяя внимание балансу интересов государства и прав личности, формированию и развитию в положительном русле цифровой культуры граждан. Особенностью национальной стратегии кибербезопасности КНР является использование термина «киберпространство» в качестве объекта регулирования. Следует рассмотреть возможность закрепления дефиниции киберпространства, используемой в КНР, в российском законодательстве. Важным аспектом китайской стратегии является определение граждан как активных субъектов информационного пространства с последующим установлением их правового статуса в отношениях обеспечения кибербезопасности и возложением на них соответствующей ответственности. Преимуществом китайской стратегии кибербезопасности является акцент на государственно-частном партнерстве, в то время как в России основная ответственность возложена на государственно-публичный сектор. Хотя подход Китая не является оригинальным (подобный подход использован также и другими зарубежными государствами, например Сингапуром), что не умаляет его результативности, необходимо рассмотреть его внедрение и в России для более активного привлечения частного сектора (деловых кругов и граждан) к обеспечению кибербезопасности.

1. Внукова Е.Ю., Курбатов А.И. Правовые аспекты информационной безопасности США и Китая // Конституционализм и государствоведение. – 2019. – № 2 (14). – С. 47–53.
2. Горян Э.В. Сотрудничество России и АСЕАН в сфере кибербезопасности: промежуточные результаты и перспективы дальнейшего развития // Вопросы безопасности. – 2018. – №6. – С. 56–70.

3. Закон Китайской Народной Республики о кибербезопасности. – Текст: электронный // pkulaw.com: [сайт]. – URL: https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html (дата обращения: 11.02. 2021).
4. Концепция стратегии кибербезопасности Российской Федерации. – Текст: электронный // Совет Федерации Федерального Собрания Российской Федерации: [сайт]. – 2014. – URL: http://council.gov.ru/services/discussions/themes/38324/ (дата обращения: 11.02.2021).
5. Кунакова М.С., Радивилов Д.С. Основные направления политики КНР в области кибербезопасности // Регионы мира: проблемы истории, культуры и политики: сборник статей международной научной конференции / под ред. А.А. Корнилова, 2017. – С. 149–155.
6. Понька Т.И., Рамич М.С. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Серия: Международные отношения. – 2020. – Т. 20, № 2. – С. 382–394.
7. Разумов Е.А. Киберсуверенитет как аспект системы национальной безопасности КНР // Россия и Китай: история и перспективы сотрудничества: материалы VII международной научно-практической конференции, 2017. – С. 707–710.
8. Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. – 2017. – № 4 (98). – С. 156–170.
9. Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты / Т.Г. Чекменёва, Б.А. Ершов, С.Д. Трубицын, А.А. Остапенко // Бюллетень социально-экономических и гуманитарных исследований. – 2020. – № 7 (9). – С. 78–97.
10. National Cyberspace Security Strategy. – Текст: электронный // Wordpress.com: [сайт]. – URL: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/ (дата обращения: 11.02.2021).

Транслитерация

1. Vnukova E. Yu., Kurbatov A. I. Pravovye aspekty informacionnoj bezopasnosti SSHA i Kitaya // Konstitucionalizm i gosudarstvovedenie. – 2019. – № 2 (14). – S. 47–53.
2. Goryan E.V. Sotrudnichestvo Rossii i ASEAN v sfere kiberbezopasnosti: promezhutochnye rezul'taty i perspektivy dal'nejshego razvitiya // Voprosy bezopasnosti. – 2018. – №6. – S. 56–70.
3. Zakon Kitajskoj Narodnoj Respubliki o kiberbezopasnosti. – Tekst: elektronnyj // pkulaw.com: [sajt]. – URL: https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html (data obrashcheniya: 11.02. 2021).
4. Koncepciya strategii kiberbezopasnosti Rossijskoj Federacii. – Tekst: elektronnyj // Sovet Federacii Federal'nogo Sobraniya Rossijskoj Federacii: [sajt]. – 2014. – URL: http://council.gov.ru/services/discussions/themes/38324/ (data obrashcheniya: 11.02.2021).
5. Kunakova M.S., Radivilov D.S. Osnovnye napravleniya politiki KNR v oblasti kiberbezopasnosti // Regiony mira: problemy istorii, kul'tury i politiki: sbornik statej mezhdunarodnoj nauchnoj konferencii / pod red. A. A. Kornilova, 2017. – S. 149–155.
6. Pon'ka T.I., Ramich M.S. Informacionnaya politika i informacionnaya bezopasnost' KNR: razvitie, podhody i realizaciya // Vestnik Rossijskogo universiteta druzhby narodov. Seriya: Mezhdunarodnye otnosheniya. – 2020. – T. 20, № 2. – S. 382–394.
7. Razumov E. A. Kibersuverenitet kak aspekt sistemy nacional'noj bezopasnosti KNR // Rossiya i Kitaj: istoriya i perspektivy sotrudnichestva: materialy VII mezhdunarodnoj nauchno-prakticheskoj konferencii, 2017. – S. 707–710.

8. Razumov E. A. Politika KNR po obespecheniyu kiberbezopasnosti // Rossiya i ATR. – 2017. – № 4 (98). – S. 156–170.
9. Strategiya Kitaya po obespecheniyu informacionnoj bezopasnosti: politicheskij i tekhnicheskij aspekty / T. G. Chekmenyova, B. A. Ershov, S. D. Trubicyn, A. A. Ostapenko // Byulleten' social'no-ekonomicheskih i gumanitarnyh issledovanij. – 2020. – № 7 (9). – S. 78–97.

Для цитирования: Горян Э.В. Нормативно-правовая основа обеспечения национальной безопасности в киберпространстве: опыт Китайской Народной Республики // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2021. – Т. 13, № 1. – С. 115–124.

For citation: Gorian E. V. The legal framework for national security in cyberspace: the outcomes of the People's Republic of China, *The Territory of New Opportunities. The Herald of Vladivostok State University of Economics and Service*, 2021, Vol. 13, № 1, pp. 115–124.

DOI https://doi.org/10.24866/VVSU/2073-3984/2021-1/115-124

Дата поступления: 12.02.2021.