Административное и муниципальное право
Правильная ссылка на статью:
Горян Э.В. — Развитие российского правового механизма кибербезопасности: «особый путь» или следование в русле международных тенденций? // Административное и муниципальное право. – 2019. – № 5. – С. 1 - 15.
DOI: 10.7256/2454-0595.2019.5.30140 URL: https://nbpublish.com/library_read_article.php?id=30140

Развитие российского правового механизма кибербезопасности: «особый путь» или следование в русле международных тенденций?

Горян Элла Владимировна

кандидат юридических наук

доцент, Владивостокский государственный университет экономики и сервиса

690014, Россия, Приморский край, г. Владивосток, ул. Гоголя, 41, каб. 5502

ella-gorjan@yandex.ru

Статья из рубрики "АДМИНИСТРАТИВНОЕ И МУНИЦИПАЛЬНОЕ ПРАВО И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Аннотация.

Объектом исследования являются отношения, возникающие при совершенствовании национального правового механизма обеспечения кибербезопасности в условиях появления киберугроз нового качества. Исследуются особенности российского нормативно-правового и институционального механизмов обеспечения информационной безопасности, определяются роль и влияние Российской Федерации на развитие международной системы безопасности информационно-компьютерных технологий. Рассматриваются и оцениваются закон об «автономном» интернете и закон о локализации данных на предмет соответствия международным тенденциям и стандартам обеспечения информационной безопасности. В данном исследовании использованы общие (системно-структурный, формально-логический и герменевтический методы) и специальные юридические методы научного познания (сравнительно-правовой и формально-юридический методы). Российская Федерация является ключевым актором развития международной системы безопасности информационно-компьютерных технологий. Развитие российского правового механизма кибербезопасности происходит по пути, по которому следуют многие государства мира. Применение модели «автономного интернета» оправдано заявленной целью, возможные злоупотребления являются ожидаемыми и устранимыми благодаря наличествующим инструментам. Российская модель локализации данных в пределах национальной юрисдикции является закономерной реакцией на киберугрозы для снижения потенциальных рисков, которые имеют место быть в современной ситуации глобализации и от которых ни одно государство не застраховано, даже если его механизм кибербезопасности считается лучшим в мире (Сингапур). На будущее российскому законодателю следует рассмотреть возможность применения мер, аналогичных тем, которые были в последние годы приняты США, Австралией и Великобританией в отношении ужесточения требований к импортируемому оборудованию, особенно в свете развития сетей поколения 5G.

Ключевые слова: кибербезопасность, критическая информационная инфраструктура, национальная безопасность, информационно-коммуникационные технологии,

автономный интернет, локализация данных, правовой механизм, телекоммуникационное оборудование, 5G сети, частный сектор

DOI:

10.7256/2454-0595.2019.5.30140

Дата направления в редакцию:

27-06-2019

Дата рецензирования:

27-06-2019

Дата публикации:

17-07-2019

Актуальность темы исследования. Последнее десятилетие характеризуется процессами по вовлечению представителей частного сектора в национальные механизмы кибербезопасности и одновременным усилением государственного контроля за их деятельностью. Наиболее ярким примером служит ситуация в Великобритании, правительство которой в 2010 году создало совместный центр с одним из ведущих производителей телекоммуникационного оборудования, компанией Huawei (КНР), - Центр оценки кибербезопасности Huawei (Huawei Cyber Security Evaluation Centre, далее - HCSEC). Он был открыт в ноябре 2010 года по соглашению между Huawei и правительством Великобритании для устранения всех потенциальных рисков, связанных с участием Huawei в формировании критической информационной инфраструктуры (далее – КИИ). HCSEC обеспечивает оценку безопасности телекоммуникационного оборудования, используемого в стране, и представляет ежегодные доклады правительству о технологиях и продуктах Huawei [1]. Деятельность HCSEC контролируется непосредственно Национальным центром кибербезопасности Великобритании (National Cyber Security Centre, NCSC). Позднее, в 2012 году, в специальном докладе для Палаты представителей США крупнейшие производители телекоммуникационного оборудования из Китая были признаны в качестве потенциальной угрозы для национальной безопасности [2] по причине подозрения в связи представителей частного сектора и правительства КНР и возможной компрометации поставляемого оборудования и технологий [3].

Но с 2018 года, когда при проведении киберучений в Австралии были выявлены возможные катастрофические для КИИ последствия атак на телекоммуникационные сети, работающие по технологии 5G, обеспокоенность государств получила реальное воплощение в мерах, которые начали предприниматься на национальном уровне – от запрета приобретения телекоммуникационного оборудования у производителей КНР (США) до ограничения сфер его применения (государства-участники ЕС). Предыдущие меры отдельных государств были направлены на «точечное» обеспечение безопасности, прежде всего, персональных данных и КИИ. Потенциальные риски, сопутствующие внедрению новых технологий, заставляют государства подходить к решению проблем

нестандартными способами, например, путем обеспечения режима «автономности» (Российская Федерация) или изоляции информационно-компьютерных сетей (КНР). Сложность оценки эффективности того или иного национального правового механизма обеспечения кибербезопасности заключается в невозможности [4] или нежелании рассматривать данное правовое явление вне политического контекста [3]. Вышесказанное и обуславливает актуальность нашего исследования.

Постановка проблемы исследования. Предпринимаемые Россией меры по обеспечению информационной безопасности как на международном, так и национальном уровне зачастую вызывают критику как со стороны политических оппонентов, так и пользователей интернета. В качестве основных аргументов выдвигаются обвинения в цензуре в форме ограничения прав и свобод пользователей, а также в государственной монополизации ключевых позиций по обеспечению работы интернета – трансграничных линий связи, технологических сетей связи, точек обмена трафиком и проч. Возникает вопрос: насколько используемый Россией механизм обеспечения кибербезопасности отличается от зарубежных, а вводимые меры – оправданы с точки зрения обеспечения общественной и национальной безопасности.

Цели и задачи исследования. Цель исследования – охарактеризовать правовой механизм информационной безопасности Российской Федерации в аспекте его соответствия угрозам последних лет. Для достижения поставленной цели определены задачи исследования, заключающиеся в определении уровня вовлеченности России в международную систему информационной безопасности и соответствия предпринимаемых мер правового и организационно-правового характера международным стандартам в этой сфере.

Методология. В данном исследовании будут использованы общие (системно-структурный, формально-логический и герменевтический методы) и специальные юридические методы научного познания (сравнительно-правовой и формально-юридический методы).

Предмет исследования, источниковая база исследования. Предмет исследования составляют нормативно-правовые акты в сфере обеспечения информационной безопасности на национальном и международном уровнях.

Выбранная нами для исследования тема мало представлена в российской научной литературе. Институциональные аспекты российского механизма обеспечения кибербезопасности рассмотрены в работах, посвященных деятельности Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК)[5], Федеральной службы безопасности Российской Федерации (далее - ФСБ)[6], Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор) [7]. Исследования зарубежных механизмов представлены весьма скудно [8].

Из зарубежных научных источников следует отметить работу, посвященную российской концепции кибербезопасности в международном и национальном аспектах [9], а также упомянуть дискуссию относительно развития национальных механизмов в ключе расширения участников до широкого представления частного сектора в них [10; 11]. Следует отметить, что для зарубежных исследователей российский механизм кибербезопасности представляет интерес прежде всего во внешнеполитическом аспекте [12].

Основная часть. Российская Федерация является инициатором создания системы международной информационной безопасности. Несмотря на то, что проблема устойчивого развития международного сообщества в эпоху информационно-компьютерных технологий (далее – ИКТ) являются предметом обсуждений уже несколько десятилетий, тем не менее, с 1998 года на рассмотрение международного сообщества ежегодно выносятся российские проекты резолюции ГА ООН «Достижения в сфере информации и телекоммуникаций в контексте международной безопасности» (Developments in the field of information and telecommunications in the context of international security) [13], поддерживаемые Индией и КНР и вызывающие острые дискуссии с США и ЕС по ключевым вопросам: цифровой суверенитет и права человека. Однако благодаря этим резолюциям была создана Группа правительственных экспертов по кибербезопасности (Group of Governmental Experts on cybersecurity, далее - GGE), которая работает в течение ряда лет (2004-2005 гг., 2009-2010 гг., 2012-2013 гг., 2014-2015 гг., 2016-2017 гг., 2018 г. - настоящее время). В 2011 году Россия и ее соратники по ШОС предложили на рассмотрение международного сообщества Международный кодекс поведения для информационной безопасности (International Code of Conduct for Information Security) [14] в форме проекта конвенции о международной информационной безопасности (Draft Convention on international information security) , но отличный от западного подход к регулированию киберпространства [9] послужил одной из причин отклонения этого документа. Тем не менее, запущенный процесс активного взаимодействия государств в рамках GGE с последующим обсуждением ежегодных докладов Генерального секретаря ООН утвердил многополярный характер международной безопасности и вывел в лидеры мнений Сингапур, Индию и КНР. Результатом работы Группы правительственных экспертов по кибербезопасности стал так называемый кодекс поведения государств в государственной сфере, охватывающий 13 норм, включенных в 2018 году в две резолюции ГА ООН: 1) принцип международного сотрудничества в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности; 2) принцип обоснованности обвинений в организации и совершении противоправных деяний, выдвигаемые против государств; 3) недопущение использования своей территории для совершения международно-противоправных деяний как субъектами международного права, так и негосударственными субъектами; 4) поиск наилучших форм сотрудничества в рассматриваемой сфере; 5) неразрывность обеспечения информационной безопасности с обеспечением прав человека; 6) принцип воздержания от деятельности в сфере ИКТ, вредной для КИИ; 7) обязанность защищать КИИ с учетом международных стандартов глобальной культуры кибербезопасности; 8) обязанность оказывать помощь друг другу в защите КИИ; 9) обязанность принимать разумные меры для обеспечения целостности каналов поставки информации; 10) обязанность предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций; 11) транспарентность действий по предотвращению и доступность информации о факторах уязвимости в сфере ИКТ; 12) обязанность воздерживаться от осуществления и поддержки деятельности в ущерб группам готовности к компьютерным инцидентам и не использовать их для злонамеренных действий; 13) вовлечение частного сектора и гражданского общества в механизм кибербезопасности (п. 1) [15].

Параллельно Российская Федерация прилагает усилия к унификации правил международной информационной безопасности на региональном и двустороннем уровне.

На региональном уровне определенные шаги были сделаны в рамках Шанхайской организации сотрудничества (подписание соглашения в 2009 году и Душанбинской декларации в 2014 году в области обеспечения международной информационной безопасности), Содружества Независимых Государств (подписание концепции в 2008 году и соглашений 2012-2013 гг.), а также Организации договора о коллективной безопасности (создание Центра по противодействию киберугрозам в 2014 году). На двустороннем уровне были подписаны соглашения в области международной информационной безопасности между Россией и Республикой Беларусь (2013), Кубой (2014), Китаем (2015), Вьетнамом (2018) и др.

На национальном уровне становление механизма обеспечения кибербезопасности происходит на уровне, сопоставимом с передовыми государствами. В частности, в 2018 году вступил в силу федеральный закон о безопасности КИИ (далее – ФЗ-187)[16], уголовное законодательство установило ответственность за посягательства на КИИ в форме неправомерного воздействия, неправомерного доступа и нарушении правил эксплуатации КИИ (ст. 274.1 Уголовного Кодекса РФ).

Следует отметить, что российский механизм обеспечения кибербезопасности КИИ согласно разработанной классификации Европейского агентства сетевой и информационной безопасности (European Union Agency for Network and Information Security, ENISA) соответствует четвертому, самому высокому уровню[17, с. 6]. Принятые за последние годы нормативно-правовые инструменты позволяют не только определить секторы КИИ, но и установить их категорию, то есть определить необходимую степень защиты [18]. В качестве недостатка, требующего скорейшего исправления, следует отметить отсутствие четких нормативных предписаний о процедуре идентификации информационных сетей как КИИ и организаций как субъектов КИИ [19, с. 55].

Институциональный механизм кибербезопасности России представлен рядом органов государственной власти общей и специальной компетенции. Президент и Правительство Российской Федерации осуществляют общую координацию деятельности органов специальной компетенции – ФСБ, ФСТЭК и Национального координационного центра по компьютерным инцидентам (далее – НКЦКИ). ФСБ осуществляет правовое регулирование деятельности НКЦКИ, осуществляющего сбор, накопление, систематизацию и анализ информации, поступающей от субъектов КИИ и ФСТЭК, а также организующего и осуществляющего обмен этой информацией как между российскими субъектами КИИ, так и между субъектами КИИ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями (п. 4.2) [20]. В свою очередь, ФСТЭК ведет реестр значимых объектов КИИ и устанавливает требования по обеспечению их безопасности, а также осуществляет государственный контроль в рассматриваемой сфере. Следует отметить федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи - Министерство цифрового развития, связи и массовых коммуникаций (в лице Роскомнадзора, далее - Минкомсвязи), который по согласованию с ФСБ утверждает порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ (ч. 5 ст. 6 ФЗ-187). Особенностью российского механизма является активное участие ФСБ - службы, располагающей специальными силами и средствами, а также наделенной процессуальными полномочиями по оперативному реагированию на кибератаки [19, с. 58].

Правовая характеристика российского механизма кибербезопасности в сравнении с ведущими государствами была дана нами в предыдущих исследованиях [19; 21]. Мы пришли к выводу, что и институциональный, и нормативный российские механизмы обеспечения кибербезопасности не уступают национальным механизмам ведущих государств (в частности, Сингапура), а даже имеют некоторые преимущества. Основные задачи кибербезопасности состоят в защите непосредственно информационных систем (прежде всего, КИИ) и данных, находящихся в них. Следовательно, государство должно обеспечить эти два объекта. Для решения первой задачи государство или ограничивает свою ответственность в пределах КИИ (так называемая «классическая» модель), или берет на себя ответственность за безопасность всех информационных систем, используя специальные организационно-правовые и технические меры (так называемая «китайская» модель). Вторая задача решаема или путем возложения ответственности за сохранность данных на самих пользователей и операторов информационных систем - «либеральная» модель, или путем введения специальных требований о локализации всех данных в пределах юрисдикции государства - модель «цифрового национализма» (data nationalism).

Рассмотрим, как российский законодатель решает указанные задачи. В мае 2019 года был принят так называемый закон об «автономном» интернете [22], разработка и принятие которого вызвали бурные дискуссии. Следует отметить, что этот закон имеет целью противостояние угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования. Однако в тексте закона не указаны виды таких угроз. Для этого разрабатывается соответствующее постановление правительства, которое содержит подробное описание угроз [23]. В частности, выделено три вида: 1) угроза целостности; 2) угроза устойчивости; 3) угроза безопасности функционирования сетей связи общего пользования.

Под угрозой целостности сетей связи общего пользования понимается угроза нарушения способности взаимодействия сетей связи, при котором становится не возможным установление соединения и (или) передача информации между пользователями услугами связи. Под угрозой устойчивости сетей связи общего пользователя понимается угроза, при которой нарушается способность сети связи сохранять свою целостность в условиях эксплуатации технических средств связи, соответствующих установленным в документации производителей, при отказе части элементов сети связи и возвращаться в исходное состояние (надежность сети связи), а также в условиях внешних дестабилизирующих воздействий природного и техногенного характера (живучесть сети связи). Под угрозой безопасности функционирования сетей связи общего пользования понимается угроза нарушения способности оператора связи противостоять попыткам несанкционированного доступа к техническим и программным средствам сети связи общего пользования и преднамеренным дестабилизирующим внутренним или внешним информационным воздействиям, следствием которых может быть нарушение функционирования сети связи (пп. 5-7 раздела II) [23].

Закон об «автономном» интернете вносит изменения в два ключевых федеральных закона: «О связи» [24] и «Об информации, информационных технологиях и о защите информации» [25]. В частности, в федеральный закон «О связи» внесена легальная дефиниция термина «точка обмена трафиком», под которым понимается совокупность технических и программных средств, сооружений связи, которые используются для соединения и пропуска в неизменном виде трафика между сетями связи, если

собственник (иной владелец) сетей связи имеет номер автономной системы (п. 28.5 ст. 2) [24]. «Номер автономной системы» также является новым для законодательства понятием, и он означает уникальный идентификатор совокупности средств связи и иных технических средств в информационно-телекоммуникационной сети «Интернет» (ч. 1 ст. 56.1) [24].

Ключевым положением закона об «автономном» интернете является применение особой технической меры обеспечения кибербезопасности, а точнее противодействия угрозам устойчивости, безопасности и целостности функционирования Интернета, - обязательная установка в сетях связи технических средств, определенных как «технические средства противодействия угрозам» (ч. 5.1 ст. 46) [24]. Данная мера сопряжена с организационно-правовой мерой, которая заключается в возложении дополнительных обязанностей на операторов связи, оказывающих услуги по предоставлению доступа к Интернету (далее - провайдеры). В частности, они обязаны установить упомянутые технические средства, а в течение трех последующих дней – предоставить информацию о фактическом месте их установки в уполномоченный орган и соблюдать технические условия установки этих технических средств и требования к сетям связи (ч. 5.1 ст. 46) [24]. Более подробные требования о порядке установки и эксплуатации технических средств противодействия угрозам, а также о модернизации сетей связи провайдерами будут утверждены соответствующим актом Правительства Российской Федерации.

Непосредственно сам механизм функционирования «автономного» интернета изложен в главе 7.1 «Обеспечение устойчивого, безопасного и целостного функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет», дополняющей федеральный закон «О связи».

Во-первых, именно на провайдеров (операторов связи, собственников (иных владельцев) технологических сетей связи, точек обмена трафиком, линий связи, пересекающих Государственную границу Российской Федерации, а также иные лица, имеющие номер автономной системы) возложена обязанность по обеспечению устойчивого, безопасного и целостного функционирования интернета в России (ч. 1 ст. 56.1) [24]. Для выполнения этой обязанности указанным субъектам необходимо приобрести практические навыки, для чего планируется проведение специальных учений (ч. 3 ст. 56.1) [24]. Представленный проект постановления правительства содержит положения о видах, целях, задачах и порядке проведения учений [26]. В частности, учения планируется проводить на федеральном и региональном уровнях (п. 2); кроме провайдеров к учениям планируется привлекать Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральную службу безопасности Российской Федерации, Министерство обороны Российской Федерации, Федеральную служба охраны Российской Федерации, Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральное агентство связи, а также иные органы государственной власти и органы местного самоуправления по решению Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (п. 3). Во время проведения учений планируется решение задач по: 1) определению и практической реализации мер по выявлению угроз информационной безопасности, целостности и устойчивости функционирования интернета с уточнением моделей таких угроз; 2) актуализации норм, обеспечивающих указанную безопасность; 3) обучению применению приемов по обеспечению устойчивости функционирования

интернета и сети связи общего пользования на территории государства; 4) исследованию и совершенствованию приемов и способов обеспечения защищенности интернета и сетей связи общего пользования (п. 5) [26].

Рассматриваемый проект постановления предусматривает основание для организации и проведения учений – утвержденный Минкомсвязи план, который должен быть согласован с ФСБ, Министерством обороны Российской Федерации, Федеральной службой охраны Российской Федерации и Министерством Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (п. 6) [26]. Такой план должен включать а) тему и замысел учений; б) цели проведения учений; в) сроки учений и их календарный план; г) органы исполнительной власти, участвующие в подготовке и проведении учений, состав руководства и посреднического аппарата учений; д) организации, привлекаемые к участию в учениях; е) масштаб проведения – федеральный/региональный уровень; ж) сети или сегменты сети, в том с эмулированным абонентским трафиком, предназначенные для проведения учений; з) перечень мероприятий по подготовке учения; и) порядок осуществления контроля за выполнением мероприятий по подготовке учения (п. 7) [26]. Состав руководства учениями и состав участников определяется приказом Минкомсвязи (п. 8) [26]. Ответственность за подготовку проведения учений возложена на Центр мониторинга и управления сетью связи общего пользования (п. 10), созданный в феврале 2019 года [27].

Кроме обязанностей по установлению технических средства противодействия угрозам и участия в учениях, провайдеры обязаны: 1) заключать договоры о передаче во владение или в пользование линии связи, пересекающей Государственную границу Российской Федерации, содержащие информацию о цели использования указанной линии связи, а также о средствах связи, установленных на указанной линии связи, с последующим предоставлением в уполномоченный орган власти информации о цели использования линии связи, а также о средствах связи, установленных на указанной линии связи (ч. 1 ст. 56.2) [24]; 2) уведомлять о начале осуществления деятельности по обеспечению функционирования точки обмена трафиком (ч. 2 ст. 56.2) [24].

Необходимо отметить такую организационно-правовую меру рассматриваемого механизма обеспечения информационной безопасности как учреждение специального реестра точек обмена трафиком (ч. 3 ст. 56.2) [24].

В случае присвоения провайдерам номера автономной системы, на них возлагаются дополнительные обязанности (ч. 8-9 ст. 56.2) [24], связанные с особенностями правового режима автономных систем, например, в случае использования точек обмена трафиком для взаимодействия с имеющими номер автономной системы провайдерами для передачи сообщений электросвязи использовать точки обмена трафиком, сведения о которых содержатся в реестре точек обмена трафиком (п. 2 ч. 8 ст. 56.2) [24]. Отдельно нужно остановиться на обязанности такого провайдера предоставлять в установленном законом порядке информацию в следующем объеме: 1) о номере их автономной системы и принадлежащих ей сетевых адресах; 2) о взаимодействии с провайдерами, имеющими номер автономной системы; 3) о местах подключения своих средств связи к линиям связи, пересекающим Государственную границу Российской Федерации, и используемых для этого технических и программных средствах; 4) о местах установки своих средств связи, подключенных к линиям связи, расположенным за пределами территории Российской Федерации; 5) о маршрутах сообщений электросвязи; 6) об инфраструктуре

своей сети связи (п. 4 ч. 8 ст. 56.2) [24]. Отдельно также указана обязанность провайдеров, имеющих номер автономной системы, в установленном законом порядке (ч. 10 ст. 56.2) [24] сотрудничать и оказывать содействие уполномоченным органам государственной власти, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации (п. 3 ч. 9 ст. 56.2) [24].

В случае возникновения угроз устойчивости, безопасности и целостности функционирования российского сегмента интернета предусмотрен особый порядок реагирования элементов институционального механизма: 1) мониторинг функционирования сетей; 2) введение централизованного управления сетью связи общего пользования (путем передачи обязательных к выполнению указаний провайдерам, участвующим в централизованном управлении); 3) предоставление на безвозмездной основе провайдерам технических средств противодействия угрозам с последующим регулированием технических условий их установки и использования (ст. 65.1) [24]. Порядок централизованного управления сетью связи общего пользования устанавливается правительством Российской Федерации и включает в себя: 1) виды угроз; 2) регламент определения угроз и меры по их устранению; 3) требования к организационно-техническому взаимодействию в рамках централизованного управления сетью связи общего пользования; 4) способы определения технической возможности исполнения указаний, передаваемых в рамках централизованного управления сетью связи общего пользования; 5) условия и случаи, при которых провайдер имеет право не направлять трафик через технические средства противодействия угрозам (п. 5 ст. 65.1) [24]. Субъекты централизованного управления обязаны выполнять установленные правила маршрутизации сообщений электросвязи (п. 6 ст. 65.1) [24]. Закон устанавливает также требование о локализации средств связи, используемых в централизованном управлении (на территории Российской Федерации) (п. 8 ст. 65.1) [24]. После вступления в силу закона об «автономном» интернете (1 ноября 2019 года), блокирование запрещенного контента будет осуществляться не силами операторов связи, как это имеет место сейчас, а Роскомнадзором.

Внесенные изменения и дополнения в федеральный закон «Об информации, информационных технологиях и о защите информации» предусматривают ряд организационно-правовых и организационно-технических мер, обеспечивающих безопасность информационно-коммуникационных систем. В частности, в статью 13 была включена часть 2.1, предусматривающая обязанность государственных и муниципальных провайдеров (операторов государственных информационных систем, муниципальных информационных систем, информационных систем юридических лиц, осуществляющих закупки в соответствии с Федеральным законом от 18 июля 2011 года №223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц») при эксплуатации информационных систем исключить использование размещенных за пределами территории Российской Федерации баз данных и технических средств, не входящих в состав таких информационных систем [25]. Любое взаимодействие субъектов публичного сектора между собой и с гражданами (физическими лицами) должно осуществляться в соответствии с правилами и принципами, установленными национальными стандартами Российской Федерации в области криптографической защиты информации (ч. 2.3 ст. 13) [25]. Данное положение вступит в силу 1 января 2021 года.

Законом об «автономном» интернете предусмотрено создание национальной системы доменных имен (совокупность взаимосвязанных программных и технических средств, предназначенных для хранения и получения информации о сетевых адресах и доменных

именах) (ч. 1 ст. 14.2) [25]. Перечень групп доменных имен, составляющих российскую национальную доменную зону, будет определен Роскомнадзором (ч. 3 ст. 14.2) [25]. Подзаконные нормативные акты регулирования этой системы находятся в стадии разработки, а положения закона вступят в силу 1 января 2021 года.

Насколько можно судить по тексту закона и наличествующим проектам подзаконных актов во исполнение его, российская модель «автономного» интернета не является «калькой» моделей КНР или КНДР, а представляет собой оригинальную модель, характеризующуюся признаком необходимого для достижения поставленной цели (защиты от определенных видов угроз) участия государства. В отличие от указанных выше государств, в России отсутствует жесткая централизация и государственная монополия на предоставление информационных услуг. В КНР государство определяет не только поставщиков услуг, но и их содержание (так называемая цензура). Более того, для «китайской» модели характерна передача функции цензуры на аутсорсинг представителям частного сектора (например, новостному агрегатору Toutiao), превращая их в квази-государственные корпорации, но обеспечивая их финансовую независимость [28]. Интернет-цензура в КНР устанавливается и регулируется тремя нормативно-правовыми актами. Временный регламент управления международной сетью информационной компьютерной связи 1996 года (Temporary Regulation for the Management of Computer Information Network International Connection) предусматривает лицензирование деятельности провайдеров и обязательное прохождение интернет-трафика через одну из сетей: ChinaNet (China Telecommunications Corporation), GBNet (Golden Bridge Network), CERNET (The China Education and Research Network) или CSTNET(China Science and Technology Network). Второй источник регулирования - Указ о защите безопасности компьютерных информационных систем 1994 года (Ordinance for Security Protection of Computer Information Systems), наделяющий полномочиями по обеспечению информационной безопасности Министерство общественной безопасности и установивший такие понятия как «вредная информация» и «вредная деятельность» в отношении интернета. Третий источник - постановление Госсовета №292 (State Council Order №292), установившее общие правила, ограничивающие деятельность интернет-провайдеров (лицензирование и отдельные разрешения для передачи данных из зарубежных СМИ). Именно статьей 11 этого указа возлагается ответственность на провайдеров за обеспечение законности любой распространяемой информации, а статья 14 предоставляет государственным должностным лицам полный доступ к любой конфиденциальной информации, которую они хотят от поставщиков интернет-услуг [29].

Как мы видим, российская модель существенно отличается от китайской. Поскольку полноценное сравнение этих моделей является объектом отдельного исследования, то сравнение общих подходов позволяет нам сделать вывод о качественном различии этих моделей, несмотря на кажущуюся схожесть. Разница заключается как в целях, так и в средствах достижения этих целей. Российская модель направлена на обеспечение безопасности российского сегмента интернета от внешних угроз, китайская же – обеспечение граждан страны «человеческой мудростью», кристаллизированной в интернете, поощряя использование Интернета способами, которые направлены на содействие экономическому и социальному прогрессу, улучшению общественных услуг и облегчению работы и жизни людей [30]. Российская модель предусматривает ситуативное реагирование на угрозы, определенные законодательством, китайская же – постоянную деятельность уполномоченных лиц по генерированию контента, одобренного руководством государства.

Тем не менее, возможно возникновение проблем, связанных со злоупотреблением инструментами «автономного» интернета как в частных интересах, так и в государственных (речь идет об опасениях либеральной части общества, что эти инструменты будут использоваться в качестве средств цензуры). Однако в первом случае существуют соответствующие механизмы правовой защиты, а во втором – необходимо достижение баланса между публичными и частными интересами, что может потребовать реформирования системы государственного контроля (надзора), благо положительный опыт Австрии и ФРГ уже имеется [7, с. 148]. При условии неуклонного и жесткого соблюдения нормативных предписаний (как буквы, так и духа закона) данный механизм способен стать важным структурным компонентом российского механизма обеспечения кибербезопасности.

В отношении защиты данных, как указывалось выше, государства идет путем или возложения ответственности за сохранность данных на самих пользователей и операторов информационных систем, устанавливая жесткие правила для провайдеров - «либеральная» модель, или путем введения специальных требований о локализации всех данных в пределах юрисдикции государства - модель «цифрового национализма» (data nationalism). Идея «цифрового национализма», одним из воплощений которой является российский закон, обязывающий операторов персональных данных при сборе персональных данных, в том числе посредством Интернета, обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории России [31], не нова для международного сообщества. Многие государства принимают так называемые законы о локализации данных (data localization laws) в том или ином объеме. Например, законодательство Нигерии устанавливает правило, по которому все правительственные данные должны были размещены в пределах ее границ; Вьетнам обязывает интернет-провайдеров хранить данные на территории государства для возможной государственной проверки; Австралия запрещает в некоторых случаях передачу данных о состоянии здоровья за границу; а специальные директивы Европейского Союза о защите данных поощряют локализацию данных в его пределах, устанавливая строгие требования в случае передачи личных данных в страны, не являющиеся членами ЕС [32]. Защита личных данных стала объектом пристального внимания законодателя Сингапура после их массовой компрометации в 2018 году, от которой пострадал и глава государства [33]. Отказ Индии от либерализции своего законодательства о локализации данных в пользу США послужило основанием для применения последними контрмер в форме ужесточения визового режима для задействованных в сфере информационных технологий специалистов [34]. Поэтому можно сделать вывод, что установление российской модели защиты данных является следованием в русле международной тенденции обеспечить национальную информационную безопасность.

Выводы. Подводя итоги нашего исследования, считаем важным отметить следующее. Развитие российского правового механизма кибербезопасности происходит по пути, по которому следуют многие государства мира. Применение модели «автономного» интернета оправдано заявленной целью, возможные злоупотребления являются ожидаемыми и устранимыми благодаря наличествующим инструментам. Российская модель локализации данных в пределах национальной юрисдикции является закономерной реакцией на киберугрозы для снижения потенциальных рисков, которые имеют место быть в современной ситуации глобализации и от которых ни одно государство не застраховано, даже если его механизм кибербезопасности считается

лучшим в мире (Сингапур). На будущее российскому законодателю следует рассмотреть возможность применения мер, аналогичных тем, которые были в последние годы приняты США, Австралией и Великобританией[35] в отношении ужесточения требований к импортируемому оборудованию, особенно в свете развития сетей поколения 5G.

Библиография

1. Huawei cyber security evaluation centre oversight board: the fifth annual report for the Cabinet Secretary from the Huawei Cyber Security Evaluation Centre Oversight Board (published 28 March 2019) [Электронный ресурс] // GOV.UK Homepage. – Режим доступа: https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019
2. Investigation of the security threat posed by Chinese telecommunications companies Huawei and ZTE: Permanent Select Committee on Intelligence report for the United States House of Representatives (published 13 September 2012) [Электронный ресурс] // U.S. House of Representatives Permanent Select Committee on Intelligence Homepage. – Режим доступа: http://intelligence.house.gov/hearing/investigation-security-threat-posed-chinesetelecommunications-companies-huawei-and-zte-0.
3. Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE: A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence (published October 8, 2012) [Электронный ресурс] // Stanford Libraries.-Режим доступа: https://searchworks.stanford.edu/view/9762611.
4. Noor E. ASEAN Takes a Bold Cybersecurity Step [Электронный ресурс] / E. Noor // The Diplomat. – Режим доступа: https://thediplomat.com/2018/10/asean-takes-a-boldcybersecurity-step/.
5. Портнова А.С. Анализ современных нормативно-методических документов ФСТЭК России в области систем обнаружения вторжений / А.С. Портнова // Безопасные информационные технологии: Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления» / Под. ред. М.А.Басараба.-2017.-С. 340-346.
6. Труфанов В.Н. Подход к созданию центров обработки персональных данных в организациях, обеспечивающих защиту государственных информационных ресурсов / В.Н. Труфанов, Д.А. Щевелев, И.В. Демидов, С.В. Совалин // Информатизация и связь.-2018.-№ 1.-С. 56-62.
7. Иванский В.П. Государственный контроль (надзор)-инструмент противодействия угрозам национальной безопасности в информационной сфере или средство защиты неприкосновенности частной жизни: соотношение частного и публичного интересов / В.П. Иванский, Г.В. Мельничук // Вестник Российского университета дружбы народов. Серия: Юридические науки.-2017.-Т. 21.-№ 1.-С. 136-152.
8. Агеев В.О. Обеспечение защиты ГИС в зарубежных и отечественных системах / В.О. Агеев, А.К. Шилов // Информационное противодействие угрозам терроризма. 2015. № 24. С. 312-315; Горян Э.В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект // Административное и муниципальное право. — 2018.-№ 9.-С.49-60.
9. Giles K. Russia’s public stance on cyberspace issues / K. Giles // 4th International Conference on Cyber Conflict (CYCON 2012).-Tallinn, 2012.-Pp. 1-13.
10. Matania E. Structuring the national cyber defence: in evolution towards a Central Cyber

Authority / E. Matania, L. Yoffe, T. Goldstein // Journal of Cyber Policy.-2017.-№ 2(1).-Pp. 16-25.

11. Farrand B. Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism / B. Farrand, H. Carrapico // Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance. – Basel: Springer International Publishing AG, 2018.-Pp.197-217.
12. Grigsby A. Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations [Электронный ресурс] / A. Grigsby // Council on Foreign Relations.-Режим доступа: https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations.
13. Developments in the field of information and telecommunications in the context of international security [Электронный ресурс] // UNODA.-Режим доступа: https://www.un.org/disarmament/ict-security/.
14. International code of conduct for information security, Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359) // United Nations Homepage.-Режим доступа: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf.
15. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: резолюция, принятая Генеральной Ассамблеей 05.12.2018 A/73/505 [Электронный ресурс] // Организация Объединенных Наций: официальный сайт. – Режим доступа: https://undocs.org/ru/A/73/505. (Developments in the field of information and telecommunications in the context of international security A/73/505 UN Homepage, https://undocs.org/en/A/73/505)
16. О безопасности критической информационной инфраструктуры Российской Федерации : федеральный закон от 26.07.2017 №187-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: www.consultant.ru/document/cons_doc_LAW_220885/.
17. Mattioli R. Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks / R. Mattioli, C. Levy-Bencheton. – Heraklion: European Union Agency for Network and Information Security (ENISA), 2014. – 43 p.
18. 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 : постановление Правительства РФ от 8 февраля 2018 г. №127 [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: www.consultant.ru/document/cons_doc_LAW_290595/.
19. Горян Э.В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект / Э.В. Горян // Административное и муниципальное право. — 2018.-№ 9.-С.49-60.
20. О Национальном координационном центре по компьютерным инцидентам (вместе с Положением о Национальном координационном центре по компьютерным инцидентам): приказ ФСБ России от 24 июля 2018 года №366 [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_306334/.
21. Горян Э.В. Идентификация объектов критической информационной инфраструктуры

в Российской Федерации и Сингапуре: сравнительно-правовой аспект // Административное и муниципальное право. — 2018.-№ 11.-С.44-56.

22. О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» : федеральный закон от 01.05.2019 №90-ФЗ [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: www.consultant.ru/document/cons_doc_LAW_323815/.
23. Об утверждении Порядка централизованного управления сетью связи общего пользования: проект постановления Правительства Российской Федерации [Электронный ресурс] // Федеральный портал проектов нормативных правовых актов. – Режим доступа: https://regulation.gov.ru/projects#npa=91558.
24. О связи: федеральный закон от 07.07.2003 №126-ФЗ (ред. от 06.06.2019) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_43224/.
25. Об информации, информационных технологиях и о защите информации: федеральный закон от от 27.07.2006 №149-ФЗ (ред. от 18.03.2019) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/.
26. Об утверждении положения о проведении учений по обеспечению устойчивого, безопасного и целостного функционирования информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования на территории Российской Федерации: проект постановления Правительства Российской Федерации [Электронный ресурс] // Федеральный портал проектов нормативных правовых актов. – Режим доступа: https://regulation.gov.ru/projects#npa=91562.
27. О Центре мониторинга и управления сетью связи общего пользования: постановление Правительства Российской Федерации от 13.02.2019 №136 [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_318786/.
28. China has the world's most centralised internet system: a perfect example of a Hamiltonian internet for maximum control [Электронный ресурс] // The Economist Homepage.-Режим доступа: https://www.economist.com/special-report/2018/06/28/china-has-the-worlds-most-centralised-internet-system.
29. Measures for the Administration of Internet Information Services (2000.09.25), [Электронный ресурс] // CECC: Freedom of Expression – Laws and Regulations.-Режим доступа: http://webarchive.loc.gov/all/20040623205930/http://www.cecc.gov/pages/virtualAcad/exp/explaws.php
30. White paper on the Internet in China (2010) [Электронный ресурс] // China Daily Homepage.-Режим доступа: http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_4.htm
31. О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях: федеральный закон от 21.07.2014 №242-ФЗ (ред. от 31.12.2014) [Электронный ресурс] // СПС «КонсультантПлюс». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_173429/.
32. Bowman C. Data Localization Laws: an Emerging Global Trend [Электронный ресурс] // JURIST – Hotline Homepageю-Режим доступа: https://www.jurist.org/commentary/2017/01/Courtney-Bowman-data-localization/.
33. Tham I. Personal info of 1.5m SingHealth patients, including PM Lee, stolen in

Singapore's worst cyber attack [Электронный ресурс] / I. Tham // The Straits Times Singapore Homepage.-Режим доступа: https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

34. Dasgupta N. Exclusive: U.S. tells India it is mulling caps on H-1B visas to deter data rules – sources [Электронный ресурс] / N. Dasgupta, A. Kalra // Reuters Homepage.-Режим доступа: https://www.reuters.com/article/us-usa-trade-india-exclusive-idUSKCN1TK2LG.
35. Botton N. 5G and National Security After Australia's Telecom Sector Security Review [Электронный ресурс] / N. Botton, H. Lee-Makiyama // ECIPE Policy Brief. – 2018.-№8. – Режим доступа: https://ecipe.org/wp-content/uploads/2018/10/TSSR-final.pdf